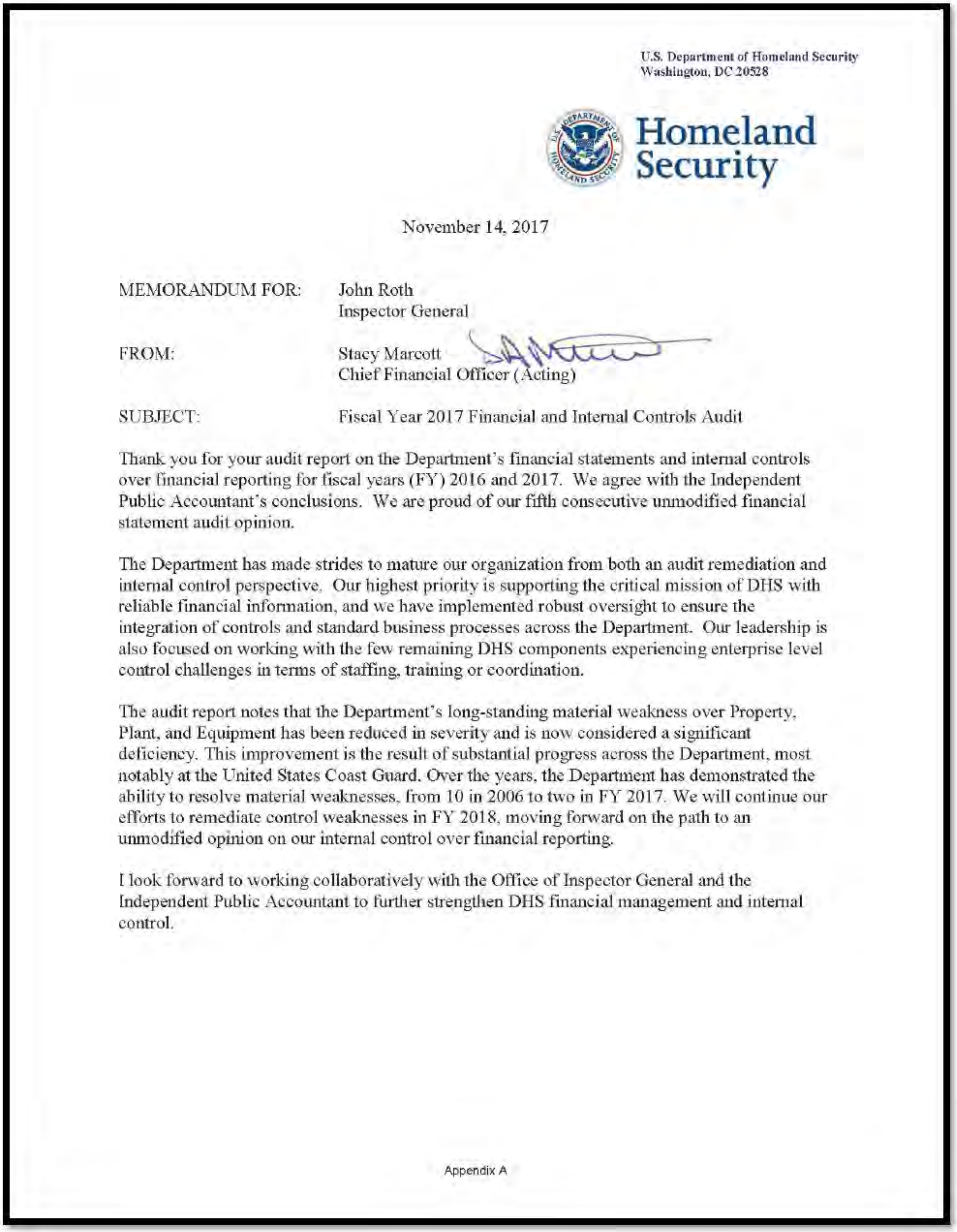


U.S. Department of Homeland Security
Washington, DC 20528

Homeland
Security

November 14, 2017

MEMORANDUM FOR: John Roth
Inspector General

FROM: Stacy Marcott
Chief Financial Officer (Acting)

SUBJECT: Fiscal Year 2017 Financial and Internal Controls Audit

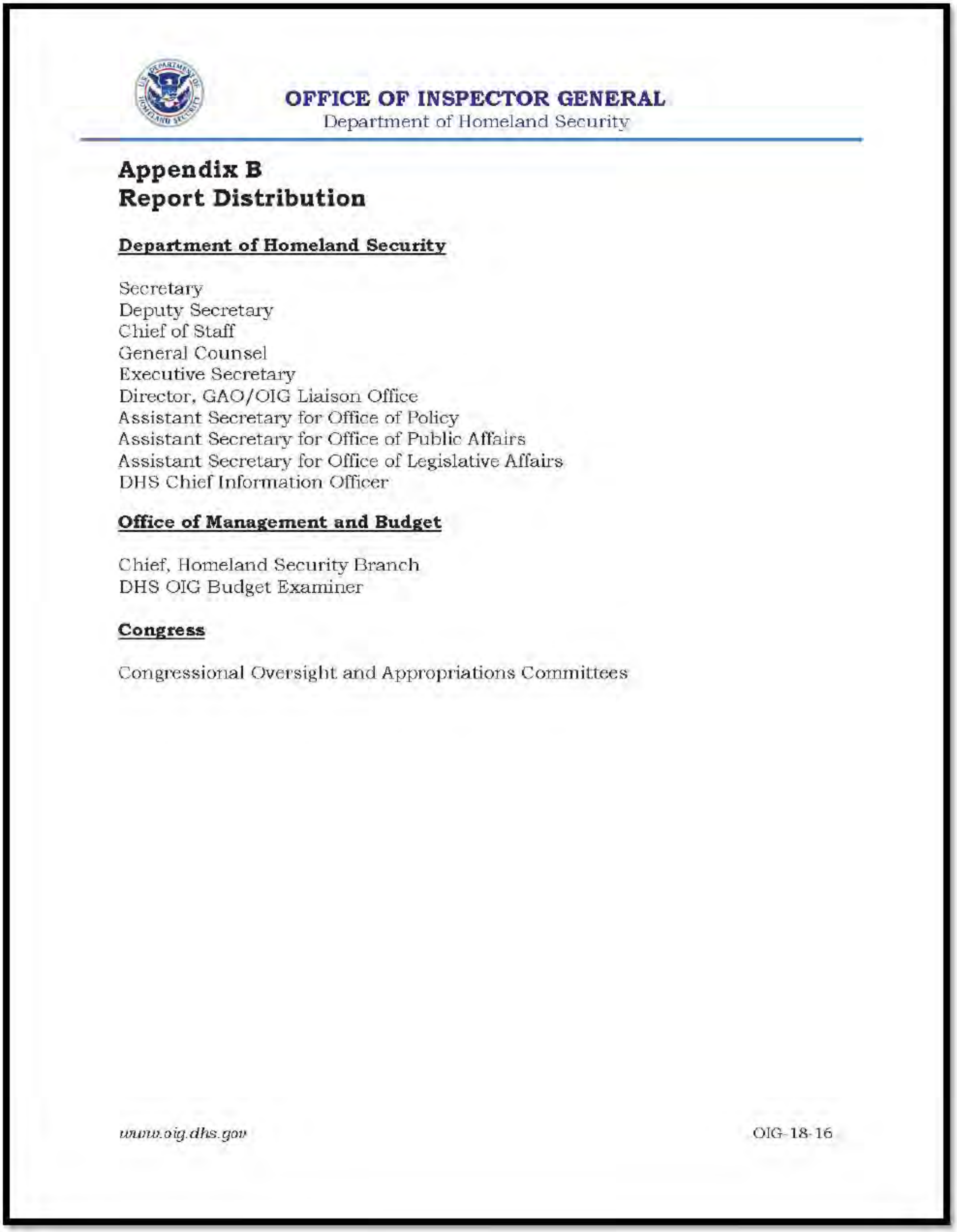
Thank you for your audit report on the Department's financial statements and internal controls over financial reporting for fiscal years (FY) 2016 and 2017. We agree with the Independent Public Accountant's conclusions. We are proud of our fifth consecutive unmodified financial statement audit opinion.

The Department has made strides to mature our organization from both an audit remediation and internal control perspective. Our highest priority is supporting the critical mission of DHS with reliable financial information, and we have implemented robust oversight to ensure the integration of controls and standard business processes across the Department. Our leadership is also focused on working with the few remaining DHS components experiencing enterprise level control challenges in terms of staffing, training or coordination.

The audit report notes that the Department's long-standing material weakness over Property, Plant, and Equipment has been reduced in severity and is now considered a significant deficiency. This improvement is the result of substantial progress across the Department, most notably at the United States Coast Guard. Over the years, the Department has demonstrated the ability to resolve material weaknesses, from 10 in 2006 to two in FY 2017. We will continue our efforts to remediate control weaknesses in FY 2018, moving forward on the path to an unmodified opinion on our internal control over financial reporting.

I look forward to working collaboratively with the Office of Inspector General and the Independent Public Accountant to further strengthen DHS financial management and internal control.

Appendix A



**OFFICE OF INSPECTOR GENERAL**
Department of Homeland Security

## Appendix B
## Report Distribution

**Department of Homeland Security**

Secretary
Deputy Secretary
Chief of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
DHS Chief Information Officer

**Office of Management and Budget**

Chief, Homeland Security Branch
DHS OIG Budget Examiner

**Congress**

Congressional Oversight and Appropriations Committees

## Additional Information and Copies

To view this and any of our other reports, please visit our website at: www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov.
Follow us on Twitter at: @dhsoig.

## OIG Hotline

To report fraud, waste, or abuse, visit our website at www.oig.dhs.gov and click on the red "Hotline" tab. If you cannot access our website, call our hotline at (800) 323-8603, fax our hotline at (202) 254-4297, or write to us at:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Hotline
245 Murray Drive, SW
Washington, DC 20528-0305

# Other Information

Citizenship Naturalization Ceremony

The ***Other Information*** section contains information on Tax Burden/Tax Gap, Combined Schedule of Spending, Summary of Financial Statement Audit and Management Assurances, Payment Integrity, Fraud Reduction, Reduce the Footprint, and Other Key Regulatory Requirements. Also included in this section are the OIG's Summary of Major Management and Performance Challenges Facing the Department of Homeland Security and Management's Response.

*Unaudited, see accompanying Auditors' Report*

# Tax Burden/Tax Gap

## *Revenue Gap*

The Entry Summary of Trade Compliance Measurement (TCM) program collects objective statistical data to determine the compliance level of commercial imports with U.S. trade laws, regulations and agreements, and is used to produce a dollar amount for Estimated Net Under-Collections, and a percent of Revenue Gap. The Revenue Gap is a calculated estimate that measures potential loss of revenue owing to noncompliance with trade laws, regulations, and trade agreements using a statistically valid sample of the revenue losses and overpayments detected during TCM entry summary reviews conducted throughout the year.

**Entry Summary of Trade Compliance Measurement**
($ in millions)

| | FY 2017 (Preliminary) | FY 2016 (Final) |
|---|---|---|
| Estimated Revenue Gap | $384.7 | $697.2 |
| Preliminary Revenue Gap of all collectable revenue for year (%) | 0.95% | 1.53% |
| Estimated Over-Collection | $44.4 | $82.8 |
| Estimated Under-Collection | $429.1 | $780.0 |
| Overall Trade Compliance Rate (%) | 99.4% | 98.9% |

The preliminary overall compliance rate for Fiscal Year (FY) 2017 is 99.4 percent. The final overall trade compliance rate and estimated revenue gap for FY 2017 will be issued in February 2018.

## Combined Schedule of Spending

The Combined Schedule of Spending (SOS) presents an overview of how departments or agencies are spending money. The SOS presents combined budgetary resources and obligations incurred for the reporting entity. Obligations incurred reflect an agreement to either pay for goods and services, or provide financial assistance once agreed upon conditions are met. The data used to populate this schedule is the same underlying data used to populate the Statement of Budgetary Resources (SBR). Simplified terms are used to improve the public's understanding of the budgetary accounting terminology used in the SBR.

**What Money is Available to Spend?** This section presents resources that were available to spend as reported in the SBR.

- ***Total Resources*** refers to total budgetary resources as described in the SBR and represents amounts approved for spending by law.
- ***Amounts Not Agreed to be Spent*** represents amounts that the Department was allowed to spend but did not take action to spend by the end of the fiscal year.
- ***Amounts Not Available to Spend*** represents amounts that the Department was not approved to spend during the current fiscal year.
- ***Total Amounts Agreed to be Spent*** represents amounts that the Department has made arrangements to pay for goods or services through contracts, orders, grants, or other legally binding agreements of the Federal Government. This line total agrees to the Obligations Incurred line in the SBR.

**How was the Money Spent/Issued?** This section presents services or items that were purchased, categorized by Components. Those Components that have a material impact on the SBR are presented separately. Other Components are summarized under Directorates and Other Components, which includes the Domestic Nuclear Detection Office (DNDO), the Federal Law Enforcement Training Center (FLETC), the Office of Intelligence and Analysis (I&A), the Office of Operations Coordination (OPS), the Management Directorate (MGMT), the Office of Health Affairs (OHA), the Office of Inspector General (OIG), the National Protection and Programs Directorate (NPPD), the Science and Technology Directorate (S&T), U.S. Citizenship and Immigration Services (USCIS), and the U.S. Secret Service (USSS).

For purposes of this schedule, the breakdown of "How Was the Money Spent/Issued" is based on the Office of Management and Budget (OMB) definitions for budget object class found in OMB Circular A-11.

- ***Personnel Compensation and Benefits*** represents compensation, including benefits directly related to duties performed for the government by federal civilian employees, military personnel, and non-federal personnel.
- ***Contractual Service and Supplies*** represents purchases of contractual services and supplies. It includes items like transportation of persons and things, rent, communications, utilities, printing and reproduction, advisory and assistance services, operation and maintenance of facilities, research and development, medical care, operation and maintenance of equipment, subsistence and support of persons, and purchase of supplies and materials.

- ***Acquisition of Assets*** represents the purchase of equipment, land, structures, investments, and loans.
- ***Grants, Subsidies, and Contributions*** represents, in general, funds to states, local governments, foreign governments, corporations, associations (domestic and international), and individuals for compliance with such programs allowed by law to distribute funds in this manner.
- ***Insurance, Refunds, and Other Spending*** represents benefits from insurance and federal retirement trust funds, interest, dividends, refunds, unvouchered or undistributed charges, and financial transfers.

**Who did the Money Go To?** This section identifies the recipient of the money, by federal and non-federal entities. Amounts in this section reflect "amounts agreed to be spent" and agree to the Obligations Incurred line on the SBR.

The Department encourages public feedback on the presentation of this schedule. Feedback may be sent via email to par@hq.dhs.gov.

**Department of Homeland Security**
**Combined Schedule of Spending**
**For the Years Ended September 30, 2017 and 2016**
**(In Millions)**

| | 2017 | 2016 |
|---|---|---|
| **What Money is Available to Spend?** | | |
| Total Resources | $ 101,963 | $ 88,113 |
| Less Amount Available but Not Agreed to be Spent | (16,598) | (10,287) |
| Less Amount Not Available to be Spent | (3,478) | (3,191) |
| **TOTAL AMOUNT AGREED TO BE SPENT** | **$ 81,887** | **$ 74,635** |
| **How Was the Money Spent/Issued?** | | |
| ***U.S. Customs and Border Protection*** | | |
| Personnel Compensation and Benefits | $ 11,107 | $ 10,866 |
| Contractual Services and Supplies | 3,948 | 3,864 |
| Acquisition of Assets | 1,372 | 1,002 |
| Insurance, Refunds, and Other Spending | 1,798 | 2,047 |
| **Total Spending** | **18,225** | **17,779** |
| ***U.S. Coast Guard*** | | |
| Personnel Compensation and Benefits | 5,526 | 5,408 |
| Contractual Services and Supplies | 4,575 | 4,396 |
| Acquisition of Assets | 1,215 | 887 |
| Grants, Subsidies, and Contributions | 115 | 43 |
| Insurance, Refunds, and Other Spending | 18 | 5 |
| **Total Spending** | **11,449** | **10,739** |

(Continued)

## Department of Homeland Security
## Combined Schedule of Spending
## For the Years Ended September 30, 2017 and 2016
## (In Millions)

| | 2017 | 2016 |
|---|---|---|
| *Federal Emergency Management Agency* | | |
| Personnel Compensation and Benefits | 1,393 | 1,225 |
| Contractual Services and Supplies | 7,101 | 2,000 |
| Acquisition of Assets | 581 | 360 |
| Grants, Subsidies, and Contributions | 8,921 | 11,427 |
| Insurance, Refunds, and Other Spending | 6,356 | 3,956 |
| **Total Spending** | **24,352** | **18,968** |
| *U.S. Immigration and Customs Enforcement* | | |
| Personnel Compensation and Benefits | 3,292 | 3,102 |
| Contractual Services and Supplies | 3,617 | 3,142 |
| Acquisition of Assets | 205 | 150 |
| Insurance, Refunds, and Other Spending | 51 | 37 |
| **Total Spending** | **7,165** | **6,431** |
| *Transportation Security Administration* | | |
| Personnel Compensation and Benefits | 4,979 | 4,794 |
| Contractual Services and Supplies | 2,429 | 2,645 |
| Acquisition of Assets | 191 | 192 |
| Grants, Subsidies, and Contributions | 80 | 84 |
| Insurance, Refunds, and Other Spending | 4 | 4 |
| **Total Spending** | **7,683** | **7,719** |
| *Directorates and Other Components* | | |
| Personnel Compensation and Benefits | 4,828 | 4,528 |
| Contractual Services and Supplies | 7,450 | 7,752 |
| Acquisition of Assets | 606 | 567 |
| Grants, Subsidies, and Contributions | 103 | 149 |
| Insurance, Refunds, and Other Spending | 26 | 3 |
| **Total Spending** | **13,013** | **12,999** |
| *Department Totals* | | |
| Personnel Compensation and Benefits | 31,125 | 29,923 |
| Contractual Services and Supplies | 29,120 | 23,799 |
| Acquisition of Assets | 4,170 | 3,158 |
| Grants, Subsidies, and Contributions | 9,219 | 11,703 |
| Insurance, Refunds, and Other Spending | 8,253 | 6,052 |
| **TOTAL AMOUNT AGREED TO BE SPENT** | **$ 81,887** | **$ 74,635** |
| **Who Did the Money Go To?** | | |
| Non-Federal Governments, Individuals and Organizations | $ 61,825 | $ 61,654 |
| Federal Agencies | 20,062 | 12,981 |
| **TOTAL AMOUNT AGREED TO BE SPENT** | **$ 81,887** | **$ 74,635** |

# Summary of Financial Statement Audit and Management Assurances

Table 3 and Table 4 below provide a summary of the financial statement audit results and management assurances for FY 2017.

**Table 3: Summary of the Financial Statement Audit**

| Audit Opinion | Unmodified | | | | |
|---|---|---|---|---|---|
| Restatement | No | | | | |
| Material Weakness | Beginning Balance | New | Resolved | Consolidated | Ending Balance |
| Financial Reporting | 1 | 0 | 0 | 0 | 1 |
| IT Controls & System Functionality | 1 | 0 | 0 | 0 | 1 |
| Property, Plant & Equipment | 1 | 0 | 1 | 0 | 0 |
| **Total Material Weaknesses** | **3** | **0** | **1** | **0** | **2** |

For FY 2017, the Independent Auditors' Report on the integrated financial statement audit identified two material weakness conditions at the Department level. Consistent with the Independent Auditor's Report, the Department is providing reasonable assurance on internal control over financial reporting, with the exception of two material weaknesses as identified in Table 4 as of September 30, 2017. Management has performed its evaluation, and the assurance is provided based upon the cumulative assessment work performed on Entity Level Controls, Financial Reporting, Budgetary Resources, Fund Balance with Treasury, Human Resources and Payroll Management, Payment Management, Insurance Management, Grants Management, Property Plant and Equipment, Revenue and Receivables, and Information Technology General Controls across the Department. DHS has remediation work to continue in FY 2018; however, no additional material weaknesses were identified as a result of the assessment work performed in FY 2017. The following table provides those areas where material weaknesses were identified and remediation work continues.

**Table 4: Summary of Management Assurances**

| EFFECTIVENESS OF INTERNAL CONTROL OVER FINANCIAL REPORTING (FMFIA SECTION 2) | | | | | |
|---|---|---|---|---|---|
| Statement of Assurance | Modified | | | | |
| Material Weakness | Beginning Balance | New | Resolved | Consolidated | Ending Balance |
| Financial Reporting | 1 | 0 | 0 | 0 | 1 |
| IT Controls & System Functionality | 1 | 0 | 0 | 0 | 1 |
| Property, Plant & Equipment | 1 | 0 | 1 | 0 | 0 |
| **Total Material Weaknesses** | **3** | **0** | **1** | **0** | **2** |
| EFFECTIVENESS OF INTERNAL CONTROL OVER OPERATIONS (FMFIA SECTION 2) | | | | | |
| Statement of Assurance | Unmodified | | | | |
| Material Weakness | Beginning Balance | New | Resolved | Consolidated | Ending Balance |
| None Noted | 0 | 0 | 0 | 0 | 0 |
| **Total Material Weaknesses** | **0** | **0** | **0** | **0** | **0** |

| COMPLIANCE WITH FEDERAL FINANCIAL MANAGEMENT SYSTEMS REQUIREMENTS (FMFIA SECTION 4) | | | | | |
|---|---|---|---|---|---|
| Statement of Assurance | Systems do not fully conform with financial system requirements | | | | |
| Non-Conformances | Beginning Balance | New | Resolved | Consolidated | Ending Balance |
| Federal Financial Management Systems Requirements, including Financial Systems Security & Integrate Financial Management Systems. | 1 | 0 | 0 | 0 | 1 |
| Noncompliance with the U.S. Standard General Ledger | 1 | 0 | 0 | 0 | 1 |
| Federal Accounting Standards | 1 | 0 | 0 | 0 | 1 |
| **Total Non-Conformances** | **3** | **0** | **0** | **0** | **3** |

| COMPLIANCE WITH SECTION 803(a) OF THE FEDERAL FINANCIAL MANAGEMENT IMPROVEMENT ACT (FFMIA) | | |
|---|---|---|
| | DHS | Auditor |
| Federal Financial Management System Requirements | Lack of compliance noted | Lack of compliance noted |
| Applicable Federal Accounting Standards | Lack of compliance noted | Lack of compliance noted |
| USSGL at Transaction Level | Lack of compliance noted | Lack of compliance noted |

# Payment Integrity

The Improper Payments Information Act of 2002 (IPIA) (Pub. L. 107-300), as amended by the Improper Payments Elimination and Recovery Act of 2010 (IPERA) (Pub. L. 111-204) and Improper Payments Elimination and Recovery Improvement Act of 2012 (IPERIA); (Pub. L. 112-248), requires agencies to review and assess all programs and activities they administer and identify those determined to be susceptible to significant improper payments, estimate the annual amount of improper payments, and submit those estimates to Congress. A program with significant improper payments (or a high-risk program) has both a 1.5 percent improper rate and at least $10 million in improper payments, or exceeds $100 million dollars regardless of the error rate. Additionally, federal agencies are required to reduce improper payments and report annually on their efforts according to OMB Circular A-123, Appendix C, *Requirements for Effective Measurement and Remediation of Improper Payments*.

The Department performs risk assessments to determine susceptibility to improper payments, testing to estimate the rates and amounts of improper payment, establishes improper payment reduction targets in accordance with OMB guidance, and develops and implements corrective actions. In addition to this report, more detailed information on the Department's improper payments and information reported in previous Agency Financial Reports (AFR) can be found at https://paymentaccuracy.gov/.

In FY 2017, the Department made significant progress to improve its processes to comply with IPERA. The Department has successfully reduced estimated improper payment rates over the years from an average estimated improper payment rate of 1.3 percent in FY 2013 to 0.89 percent in FY 2017. In FY 2017, the OIG conducted an annual audit to determine whether the Department complied with IPERA as reported in the FY 2016 AFR. The OIG concluded DHS did not fully comply because it did not meet its annual reduction targets established by within 0.1 percent for seven of 15 programs deemed susceptible to significant improper payments. For FY2017 reporting, DHS met established reduction targets for eight of the ten programs deemed susceptible to significant improper payments due to continued corrective action efforts and sustained internal controls. We remain strongly committed to ensuring our agency's transparency and accountability to the American taxpayer and achieving the most cost effective strategy on the reduction of improper payments.

## *1. Risk Assessments*

In accordance with IPERA Section 2(a), agency heads are required to periodically review all programs and activities that the relevant agency head administers and identify all programs and activities that may be susceptible to significant improper payments, and perform the review at least once every three years.

In FY 2017, the Department established a two part process comprised of a preliminary assessment followed by a comprehensive assessment if necessary. The preliminary risk assessment process is used on all programs not already reporting an improper payment estimate. The comprehensive risk assessment process is required based on the preliminary risk assessment results and the program's three year risk assessment cycle.

In FY 2017, the Department conducted preliminary risk assessments on 83 programs. Additionally, resulting from the preliminary assessments or the three year risk assessment cycles, we conducted 35 comprehensive risk assessments. The Department assessed all payment types except for federal intragovernmental payments, which were excluded based on the definition of an improper payment per OMB Circular A-123, Appendix C.

In conducting the comprehensive risk assessments, components held meetings with program managers, key personnel, and other stakeholders to discuss the inherent risk of improper payments. The Department's comprehensive risk assessment involved evaluating attributes that directly or indirectly affect the likelihood of improper payments using the GAO Standards for Internal Control (Green Book) framework: As required by OMB Circular A-123, Appendix C, the following minimum risk factors were also considered:

- Whether the program or activity reviewed is new to the agency;
- The complexity of the program or activity reviewed, particularly with respect to determining correct payment amounts;
- The volume of payments made annually;
- Whether payments or payment eligibility decisions are made outside of the agency, for example, by a state or local government, or a regional Federal office;
- Recent major changes in program funding, authorities, practices, or procedures;
- The level, experience, and quality of training for personnel responsible for making program eligibility determinations or certifying that payments are accurate;
- Inherent risks or improper payments due to the nature of agency programs or operations;
- Significant deficiencies in the audit reports of the agency including, but not limited to, the agency Inspector General or the GAO audit report findings, or other relevant management findings that might hinder accurate payment certification; and
- Results from prior improper payment work.

Program managers and Component's internal controls division assigned a risk rating to each risk factor based on their detailed understanding of the processes and risk of improper payment. Weighted percentages were assigned to each risk factor rating based on a judgmental determination of the direct or indirect impact on improper payments. An overall risk score was then computed for each program, calculated by the sum of the weighted scores for each risk factor and overall rating scale. Programs were assessed using both qualitative and quantitative risk factors to determine if they were susceptible to significant improper payments. A weighted average of 65 percent for qualitative factors and 35 percent for quantitative risk yields the program's overall risk score.

Additionally, the Department conducted independent reviews of component submissions to identify significant changes in the program compared to last year and assess the reasonableness of the risk ratings. RM&A maintains the final documentation of component submissions and reviews, including maintaining a list of all programs and activities assessed this current FY.

## 2. Sampling and Estimation

The Department used a statistically valid, stratified sample design performed by a statistician to select and test FY 2016 disbursements for those programs identified as susceptible to significant improper payments. Our procedures provided an overall estimate of the percentage of improper payment dollars within ±2.5 percent precision at the 90 percent confidence level, as specified by OMB Circular A-123 Appendix C.

Using a stratified random sampling approach, payments were grouped into mutually exclusive "strata," or groups based on total dollars. A stratified random sample typically required a smaller sample size than a simple random sample to meet the specified precision goal at any confidence level. Once the overall sample size was determined, the individual sample size per stratum was determined using the Neyman Allocation method.
The following procedure describes the sample selection process:

- Grouped payments into mutually exclusive strata;
- Assigned each payment a random number generated using a seed;
- Sorted the population by stratum and random number within stratum; and
- Selected the number of payments within each stratum (by ordered random numbers) following the sample size design. For the certainty strata, all payments are selected.

To estimate improper payment dollars for the population from the sample data, the stratum-specific ratio of improper dollars (gross, underpayments, and overpayments, separately) to total payment dollars was calculated. The Federal Emergency Management Agency (FEMA) Homeland Security Grant Program (HSGP), and Public Assistance (PA) Program used an OMB approved alternative sampling methodology for multi-year targeted sampling plan due to population size.

## 3. Payment Reporting

The table below summarizes Improper Payment (IP) amounts for DHS programs susceptible to significant improper payments. It provides a breakdown of estimated IP and reduction targets for each DHS program or activity. IP percent (IP%) and IP dollar (IP$) results are provided from this year's testing of FY 2016 payments. Data for projected future−year improvements is based on the timing and significance of completing corrective actions.

## Table 5: Improper Payment Results and Reduction Outlook

($ in millions)

| Program Name | FY 2016 Outlays ($M) | FY 2016 IP Amount ($M) | FY 2016 IP Rate (%) | FY 2017 Outlays ($M) | FY 2017 Proper Amount ($) | FY 2017 Proper Rate (%) | FY 2017 IP Amount ($M) | FY 2017 IP Rate (%) | FY 2017 Over-payment Amount ($) | FY 2017 Over-payment Rate (%) | FY 2017 Under-payment Amount ($) | FY 2017 Under-payment Rate (%) | FY 2018 Est. IP Rate (%) & Reduction Target |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 2016 Testing (Based on FY 2015 Actual Data) | | | 2017 Testing (Based on FY 2016 Actual Data) | | | | | | | | | 2018 Testing (Based on FY 2017 Actual Data |
| Customs and Border Protection (CBP) – Refund and Drawback (R&D)[8] | $3,008.78 | $10.52 | 0.35% | $1,875.0482 | $1,860.2000 | 99.21% | $14.8443 | 0.79% | $14.8442 | 0.79% | $0.0001 | 0.00% | 0.24% |
| CBP – Administratively Uncontrollable Overtime (AUO)[4,8] | $172.99 | $0.01 | 0.01% | | | | | | | | | | |
| Domestic Nuclear Detention Office (DNDO) – Hurricane Sandy Payments[5] | $0.06 | $0.00 | 0.00% | | | | | | | | | | |
| Federal Emergency Management Agency (FEMA) – Assistance to Firefighters Grant Program (AFG)[3] | $270.91 | $2.29 | 0.85% | $299.1566 | $298.8985 | 99.91% | $0.2581 | 0.09% | $0.2581 | 0.09% | $0.0000 | 0.00% | 0.09% |
| FEMA – Flood Risk Map & Risk Analysis (FRM&RA)[6,8] | $111.52 | $6.11 | 5.48% | $132.0186 | $127.6980 | 96.73% | $4.3206 | 3.27% | $4.3201 | 3.27% | $0.0005 | 0.00% | 5.00% |
| FEMA – Homeland Security Grant Program (HSGP)[2,3] | $658.63 | $2.77 | 0.42% | $1,280.1709 | $1,275.3063 | 96.62% | $4.8646 | 0.38% | $4.8644 | 0.38% | $0.0002 | 0.00% | 0.35% |
| FEMA – National Flood Insurance Program (NFIP)[3,8] | $932.48 | $1.38 | 0.15% | $2,339.8225 | $2,339.5308 | 99.99% | $0.2917 | 0.01% | $0.2917 | 0.01% | $0.0000 | 0.00% | 0.17% |
| FEMA – Port Security Grant Program (PSGP)[4,8] | $121.57 | $1.14 | 0.94% | | | | | | | | | | |
| FEMA – Transit Security Grant Program (TSGP)[4,8] | $211.06 | $1.49 | 0.71% | | | | | | | | | | |
| FEMA – Public Assistance (PA) Program[2] | $4,198.30 | $57.10 | 1.36% | $3,410.7482 | $3,376.6407 | 99.00% | $34.1075 | 1.00% | $34.1075 | 1.00% | $0.0000 | 0.00% | 1.00% |
| FEMA – Vendor Pay (VP) | $581.51 | $31.43 | 5.40% | $974.1092 | $931.0669 | 95.58% | $43.0423 | 4.42% | $42.8922 | 4.40% | $0.1501 | 0.00% | 4.00% |
| Immigration and Customs Enforcement (ICE) – Enforcement | $1,616.01 | $5.75 | 0.36% | $1,828.1754 | $1,822.1350 | 99.67% | $6.0404 | 0.33% | $6.0368 | 0.33% | $0.0036 | 0.00% | 1.00% |

| Program Name | FY 2016 Outlays ($M) | FY 2016 IP Amount ($M) | FY 2016 IP Rate (%) | FY 2017 Outlays ($M) | FY 2017 Proper Amount ($) | FY 2017 Proper Rate (%) | FY 2017 IP Amount ($M) | FY 2017 IP Rate (%) | FY 2017 Over-payment Amount ($) | FY 2017 Over-payment Rate (%) | FY 2017 Under-payment Amount ($) | FY 2017 Under-payment Rate (%) | FY 2018 Est. IP Rate (%) & Reduction Target |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 2016 Testing (Based on FY 2015 Actual Data) | | | 2017 Testing (Based on FY 2016 Actual Data) | | | | | | | | | 2018 Testing (Based on FY 2017 Actual Data |
| and Removal Operations (ERO)[7] | | | | | | | | | | | | | |
| Office of Inspector General (OIG) – Hurricane Sandy Payments[5] | $0.17 | $0.003 | 1.76% | | | | | | | | | | |
| Science and Technology (S&T) – Hurricane Sandy Payments[1] | $2.08 | $0.00 | 0.00% | $0.7017 | $0.7017 | 100.00% | $0.0000 | 0.00% | $0.0000 | 0.00% | $0.0000 | 0.00% | 0.00% |
| United States Coast Guard (USCG) – Acquisition, Construction, & Improvements (AC&I), Operating Expenses (OE) - Hurricane Sandy | $70.00 | $0.46 | 0.66% | $79.4812 | $78.3872 | 98.62% | $1.0940 | 1.38% | $1.0940 | 1.38% | $0.0000 | 0.00% | 0.50% |
| TOTAL[9] | $11,956.07 | $120.45 | 1.01% | $12,219.43 | $12,110.57 | 99.11% | $108.86 | 0.89% | $108.71 | 0.89% | $0.15 | 0.00% | 0.97% |

Note 1: All FY 2016 Hurricane Sandy Disbursements were tested in FY 2017.

Note 2: FEMA has two State-Administered Programs, HSGP and PA, that are tested on a three-year cycle. To calculate the national error rate for FY 2016 actual data, error rate from the States tested in FY 2014, FY 2015, and FY 2016 were applied to the FY 2016 State payment populations to derive a national average. Estimated outlays for FEMA programs were calculated by averaging the total disbursements for the past three fiscal years, due to the volatile nature of the programs tested. This alternative sampling and estimation method was previously approved by OMB.

Note 3: FEMA – NFIP met the IPERA statutory threshold of below 1.5% and $10M. FEMA exceeded the goal by being below 1% for AFG, HSGP, and NFIP as well as having an extrapolated error amount below $5M for these programs. The FY 2018 estimated error rates remained consistent with the FY 2017 reported error rates. The cost to implementing additional internal controls to try to further reduce the improper payment rate would far outweigh the benefit.

Note 4: During FY 2017 OMB issued the program a waiver from further improper payment testing due to two consecutive years of low improper payment rates. The program will undergo a comprehensive risk assessment beginning FY 2018.

Note 5: Program did not record Hurricane Sandy related outlays in FY 2016, also the program does not have any remaining Hurricane Sandy funds therefore this program will not be tested in future years.

Note 6: FEMA – FRM&RA - Reduction target for out years increased from CY IP percentages. Due to the historical challenges relating to connecting invoice amounts to respective contracts, the target rate for FY 2018 is maintained at 5% as reported in FY 2016 AFR. Resolving the contract management weaknesses within the FRM program requires a methodical and thorough review, resulting in an extended timeline for this program.

Note 7: ICE – ERO implemented successful remediation actions from FY 2013 through FY 2015. The impact and focus on remediation is evidenced by the decreased improper payment rate of 0.36% for FY 2015 disbursements and 0.33% for FY 16 disbursements. Based on several years of historical improper payment rates around 4%, with the goal of reducing improper payments, ICE projects the improper payment to be 1%. While ICE has maintained a significantly low improper payment rate for two consecutive years, targeting a 1% improper payment rate in FY 18 is reasonable and achievable due to the dollar amount of the invoices in the ERO Program.

Note 8: Several corrections were made to the FY 2016 reported outlays and improper payment percentages as a result of the OIG IPERA audit (OIG 17-59). Specifically, CBP (Refunds and Drawback, Administratively Uncontrollable Overtime) and FEMA (Flood Risk Map & Risk Analysis, National Flood Insurance Program, Port Security Grant Program, and Transit Security Grant Program) program outlays and improper payment percentages were updated using the sampling frame used by the statisticians to sample and extrapolate results, rather than disbursement captured for Program ID deliverable purposes. Lastly, the Department made corrections to the program name for Hurricane Sandy funds disbursed for USCG. The outlays and improper payment percentage corrections were submitted to OMB on June 29, 2017, after the AFR was published.

Note 9: The total of estimates does not represent a true statistical improper payment estimate for the Department.

Upon analysis, we found that 55 percent of improper payments for the programs tested in FY 2017 were due to administrative or process error and 45 percent due to insufficient documentation. In addition, approximately 70 percent of improper payments were attributed to errors made by the Federal Agency and 30 percent due to errors made by State and Local Agencies and Other Parties combined. The root causes were identified through improper payment testing and categorized using categories of error as defined in the October 2014 update to OMB Circular A-123, Appendix C.

Table 6 summarizes, by program, the root cause and estimated amount of improper payments made directly by the Government, and the amount of improper payments made by recipients of Federal money for the current fiscal year.

**Table 6: Root Cause of Improper Payments**

($ in millions)

| Program Name | Payment Type | Error Made by Federal Agency | | Error Made by State and Local Agency | Error Made by Other Party[1] | TOTAL |
|---|---|---|---|---|---|---|
| | | Administrative or Process Error | Insufficient Documentation to Determine | Administrative or Process Error | Administrative or Process Error | |
| CBP – R&D | Overpayments | $14.8442 | $0.0000 | $0.0000 | $0.0000 | $14.8442 |
| | Underpayments | $0.0001 | $0.0000 | $0.0000 | $0.0000 | $0.0001 |
| FEMA - AFG | Overpayments | $0.0000 | $0.2581 | $0.0000 | $0.0000 | $0.2581 |
| | Underpayments | $0.0000 | $0.0000 | $0.0000 | $0.0000 | $0.0000 |
| FEMA – FRM & RA | Overpayments | $0.1871 | $4.1330 | $0.0000 | $0.0000 | $4.3201 |
| | Underpayments | $0.0005 | $0.0000 | $0.0000 | $0.0000 | $0.0005 |
| FEMA - HSGP | Overpayments | $0.0000 | $4.8644 | $0.0000 | $0.0000 | $4.8644 |
| | Underpayments | $0.0002 | $0.0000 | $0.0000 | $0.0000 | $0.0002 |
| FEMA - NFIP | Overpayments | $0.0000 | $0.0000 | $0.0000 | $0.2917 | $0.2917 |
| | Underpayments | $0.0000 | $0.0000 | $0.0000 | $0.0000 | $0.0000 |
| FEMA - PA | Overpayments | $1.2517 | $0.0000 | $32.8558 | $0.0000 | $34.1075 |
| | Underpayments | $0.0000 | $0.0000 | $0.0000 | $0.0000 | $0.0000 |
| FEMA - VP | Overpayments | $2.7999 | $40.0900 | $0.0000 | $0.0000 | $42.8922 |
| | Underpayments | $0.1501 | $0.0000 | $0.0000 | $0.0000 | $0.1501 |
| ICE - ERO | Overpayments | $6.0368 | $0.0000 | $0.0000 | $0.0000 | $6.0368 |
| | Underpayments | $0.0036 | $0.0000 | $0.0000 | $0.0000 | $0.0036 |
| S&T - Sandy | Overpayments | $0.0000 | $0.0000 | $0.0000 | $0.0000 | $0.0000 |
| | Underpayments | $0.0000 | $0.0000 | $0.0000 | $0.0000 | $0.0000 |
| USCG – Acquisition, Construction, & Improvements, Operating Expenses - Hurricane Sandy | Overpayments | $1.0940 | $0.0000 | $0.0000 | $0.0000 | $1.0940 |
| | Underpayments | $0.0000 | $0.0000 | $0.0000 | $0.0000 | $0.0000 |
| DHS TOTAL | | $26.37 | $49.35 | $32.86 | $0.29 | $108.86 |

[1] Other Party to include: participating lender, health care provider, or any other organization administering Federal dollars

## *4. Improper Payment Corrective Actions*

The following table lists corrective actions for the FEMA Vendor Pay (VP) program which exceeds the statutory threshold of 1.5 percent improper rate and $10 million in improper payments. These corrective actions are targeted at addressing the root causes of insufficient documentation, specifically the billed price within invoices not being identified in the contracts. The root causes of these errors are reoccurring from prior years, and FEMA has continued implementing the following corrective actions to ensure greater compliance. Through these actions, FEMA has made progress to reduce improper payments by 0.98 percentage points in 2017.

**Table 7: Vendor Payment Program Corrective Actions**

| Error Cause | Error Cause Subcategory | Corrective Actions | Completion Date |
|---|---|---|---|
| Improve quality of contracts | | | |
| Insufficient Documentation | Billed Price vs. Contract Validation | Draft and incorporate standardized billing instructions to be included in all contracts, defining the standard form and content of billings for different contract types. Incorporate standard billing instructions in contract writing system. | Completed - August 2015 |
| | | Revise contract template to include standard section for authorized invoice approver, designated payment office, and authorized official for receiving and acceptance. | Completed - August 2015 |
| | | FEMA OCPO to issue policy guidance regarding required CLIN structure to be included in contracts. | Completed - November 2015 |
| | | FEMA OCPO to train CO's as part of PRISM implementation, in uploading and maintaining Attachments or Quotes for which pricing is based, into the official contract file in PRISM. | Completed - March 2017 |
| | | FEMA OCPO to issue policy guidance requiring Attachments or Quotes incorporated by referenced to be included as part of the official contract document and maintained in the electronic contract file. | 3/31/2018 |
| Improve quality of invoice review | | | |
| Administrative or Process Error | Billed Pricing not in Contract | Conduct mandatory training for all Contracting Officer Representatives (CORs) and COs on proper invoice review and approval. | Completed training module 7/2013. Training ongoing/quarterly |
| | | Develop invoice review checklist addressing payments of different types, and what needs to be validated based on payment type. | Completed - 3/31/2017 |
| | Calculation Error; Interest Not Paid; Discount not taken | Conduct training for Vendor Payment Accounting technicians on proper review of invoices and related invoice processing. | Completed - May 2016 |

| Error Cause | Error Cause Subcategory | Corrective Actions | Completion Date |
|---|---|---|---|
| Improve quality of Receipt and Acceptance | | | |
| Administrative or Process Error | Missing Documentation | Develop a standard Inspection, Acceptance and Receiving Report for FEMA COTR's for support of invoices. | Completed - January 2016 |
| | | Develop COR specific training on documenting acceptance where required, by contract line item or deliverable. | 3/31/2018 |

## 5. Accountability

The goals and requirements of IPERIA were communicated to all levels of staff throughout the Office of the Chief Financial Officer and to relevant program office and procurement staff. The Department has taken extensive measures to ensure that managers, accountable officers (including Component CFOs), programs, and states and localities are held accountable for reducing and recapturing improper payments. The Department's CFO and senior staff have incorporated improper payment reduction targets in their annual performance plans.

Component managers are responsible for completing internal control work on payment processing as part of the Department's OMB Circular A-123 effort. They are further responsible for establishing and maintaining sufficient internal controls, including a control environment that prevents improper payments from being made, effectively managing improper payment risks, and promptly detecting and recovering any improper payment that may occur. Management's improper payments efforts are subject to an annual compliance review by the DHS's Office of Inspector General.

## 6. Agency Information Systems and Other Infrastructure

OMB requires the identification of all programs with improper payments exceeding the statutory thresholds defined as 1) both 1.5 percent of program outlays and $10 million or 2) $100 million, regardless of the improper payment percentage of total program outlays. Using this criteria, the FEMA Vendor Pay program exceeded the statutory threshold with an estimated improper payment rate of 4.42 percent and $42.89 million in estimated improper payments. Refer to Table 5: *Improper Payment Results and Reduction Outlook* for the statistically valid estimate of the annual amount of improper payment for FEMA Vendor Pay.

The Department and FEMA has the necessary internal controls, human capital, information systems, and infrastructure to continue its efforts of reducing improper payments and increase recoveries as demonstrated through reduction of estimated improper payment rates reported this FY. The Department monitors Component improper payment testing in accordance with OMB Circular A-123. Additionally, each CFO provides an annual assurance statement attesting to the effectiveness of program controls within their Component.

## 7. Barriers

There are no statutory or regulatory barriers that will impact the ability of DHS to successfully complete corrective actions to reduce improper payments.

## *8. Recapture of Improper Payments*

During FY 2017, the Department did not have any recovery audit activities for FY 2016 disbursements. The Department conducted multiple cost analysis reviews over the past several years and determined that payment recapture audit programs are not cost-effective by considering recovery amounts, costs of audits exceeding recovery amounts identified for recapture and no major changes to payment operations to justify performing an audit.

The table below identifies FY 2016 funds recovered outside of the recapture audit program. Overpayments identified through grant and contract closeout processes, IPERA testing, or self-reported by vendors were collected through the high dollar overpayment reporting process.

**Table 8: Overpayment Payment Recaptured with and without Recapture Audit Programs**

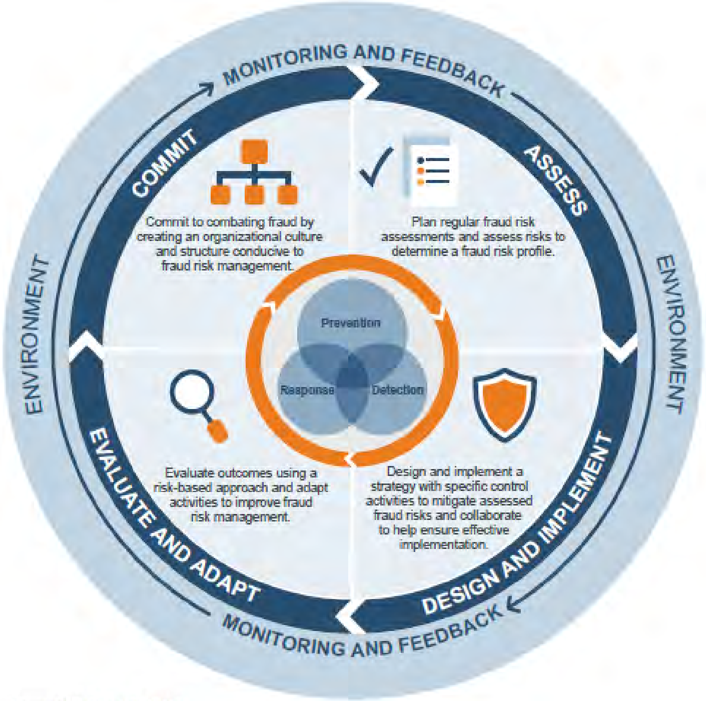
($ in millions)

| | Overpayments Recaptured outside of Payment Recapture Audits | |
|---|---|---|
| Component | Amount Identified | Amount Recaptured |
| FEMA | $0.12 | $0.00 |
| TSA | $0.83 | $0.83 |
| USSS | $0.17 | $0.17 |
| DHS Totals | $1.12 | $1.00 |

## Fraud Reduction

On June 30, 2016, Congress enacted Public Law 111-186, Fraud Reduction and Data Analytics Act (FRDAA). The FRDAA requires agencies to conduct an evaluation of fraud risks and use a risk-based approach to design and implement financial and administrative control activities to mitigate identified fraud risks; collect and analyze data from reporting mechanisms on detected fraud to monitor fraud trends and continuously improve fraud detection through use of data analytics; and use the results of monitoring, evaluation, audits and investigations to improve fraud prevention, detection and response.

DHS implemented several initiatives to comply with the FRDAA using GAO's Fraud Risk Framework and A-123. While DHS components and respective programs have individually mitigated the risk of fraud, full implementation of a Department-wide fraud management framework is an iterative process as DHS continues to build upon enterprise risk management.


MONITORING AND FEEDBACK
COMMIT
ASSESS
Commit to combating fraud by creating an organizational culture and structure conducive to fraud risk management.
Plan regular fraud risk assessments and assess risks to determine a fraud risk profile.
ENVIRONMENT
ENVIRONMENT
Prevention
Response
Detection
Evaluate outcomes using a risk-based approach and adapt activities to improve fraud risk management.
Design and implement a strategy with specific control activities to mitigate assessed fraud risks and collaborate to help ensure effective implementation.
EVALUATE AND ADAPT
DESIGN AND IMPLEMENT
MONITORING AND FEEDBACK

Source: GAO. | GAO-15-593SP

**Figure 5: GAO's Fraud Risk Framework**

To-date, DHS has completed the initial fraud risk assessment, while continuously improving our existing processes. Specifically, DHS implementation status and accomplishments include the following:

- ***Commit:*** Leadership and all levels of the organization have committed to continuously identify, prevent, detect, and respond to fraud risks, while actively engaging the OIG to assist the Department in combatting fraud. Leadership commitment, in a holistic risk management approach, is evidenced through each of the components entity level control evaluations where assessments are made based on tone at the top and integrity and ethical values. Currently, RM&A is leading the financial and administrative fraud risk management initiatives for the Department with strong support from components, while engaging the enterprise risk management work group to expand communication and awareness of fraud risk programs DHS-wide.

- ***Assess:*** As part of the Department's internal control evaluation, components are required to assess fraud risk on an annual basis to support its entity level control assessments, as prescribed within the Green Book (Principle 8, Assess Fraud Risks). In FY 2016, the Department led identifying fraud risks common to payroll, grants, payments (to include large contracts), and purchase and travel cards. Each component was required to assess the likelihood and impact of each fraud risk based on its control environment to create its financial and administrative fraud risk profile. In addition, Components were highly encouraged to identify other fraud risks that are specific for their mission and include them into its fraud risk inventory for consolidation.
- ***Design and Implement:*** For each identified fraud risk, components were required to identify control activities, leveraging work already performed through existing internal control evaluations while ensuring the mapped control activities address the fraud risk.
- ***Evaluate and Adapt:*** Once control activities were mapped or new control activities were identified, components were required to complete test of effectiveness. The results of testing would yield a residual risk rating by fraud risk/control, which is used to inform if the controls are effectively designed to mitigate the fraud risk or additional control activities are needed.
- ***Monitoring and Feedback:*** The Department, under the Chief Financial Officer (CFO), monitors the evaluations conducted by each component. Components were asked to baseline its understanding of its fraud risks and control activities in FY 2016 and FY 2017. Effective FY 2018, the Department will focus its monitoring in evaluating each component's fraud risk assessments, identify fraud risks that maybe pervasive Department-wide, and determine if the control activities are appropriate to mitigate or reduce high fraud risks. This initiative will enable the Department to identify opportunities to standardize controls, when appropriate and create synergies where data analytics can be most effectively used to monitor high risk areas. Furthermore, RM&A will continue to work with the enterprise risk management work group to communicate and expand on the awareness and implementation of fraud reduction measures, as needed.

As part of continuous improvement, DHS continues to refine fraud risks by actively working with the fraud working group hosted by OMB, continuing to research and identify additional fraud risks and schemes that need to be included into DHS' fraud risk management framework and exploring data analytic options for payments. In addition, USCIS and ICE have implemented a purchase card data analytics program that enable these component to review 100 percent of its purchase card transactions monthly and target high risk transactions for further review. As the charge card program transitions to GSA SmartPay®3, the Department will assess applicability of data analytics to the entire program to prevent and detect unusual transactions early and target high risk transactions for review and trending.

Other supporting initiatives include:

- *Contract award, monitoring and oversight* – Embedded within Federal Acquisition Regulations and the Homeland Security Acquisition Manual are measures to identify indicators of procurement fraud, and internal controls to prevent such fraud. OCPO monitors compliance with acquisition regulations and DHS policy across the Department, through its procurement oversight program. In addition, OCPO has an established Industry engagement and communication program, providing an external control for detecting fraud.

- *Improper Payments* – In accordance with IPERA, OMB requires programs identified as susceptible improper payments to be tested and the root causes of improper payments include an analysis of potential for fraudulent activity. As part of reporting efforts, Components are required to report if any potential fraudulent activity occurred and refer these matters appropriately.

## *Individual and Household Program Fraud Data Analytics*

In response to the fraud associated with Hurricanes Katrina and Rita, FEMA established the Fraud and Internal Investigations Division (FIID), located at FEMA's headquarters in Washington DC. FIID's mission includes identifying, mitigating, and preventing fraudulent losses of federal funds and assets through agency fraud awareness training and recoupment of losses in partnership with the DHS OIG.

One of FIID's responsibilities is to identify best practices to prevent and deter fraud, waste, and abuse in FEMA's delivery of disaster assistance using disaster applicant datasets to identify current fraud trends and the most common indicators of fraud, while continuing to seek new, innovative, and more effective ways to combat fraud, waste, and abuse using social media. Since its inception, FIID has shifted its approach for combating fraud from a reactive to a proactive, preventative model. FIID coordinates and shares information with the different FEMA program offices as well as personnel located at all three National Processing Service Centers (NPSC). Using that information, FIID proactively queries FEMA databases (datamining) for applications containing common indicators of fraud and identifies fraudulent applications. After identifying a fraudulent application, FIID locks the applicant's file in order to prevent fraudulent funds from being disbursed. Using this proactive model, FIID has seen a dramatic increase in the amount of fraudulent funds prevented from disbursement as seen in the chart below.

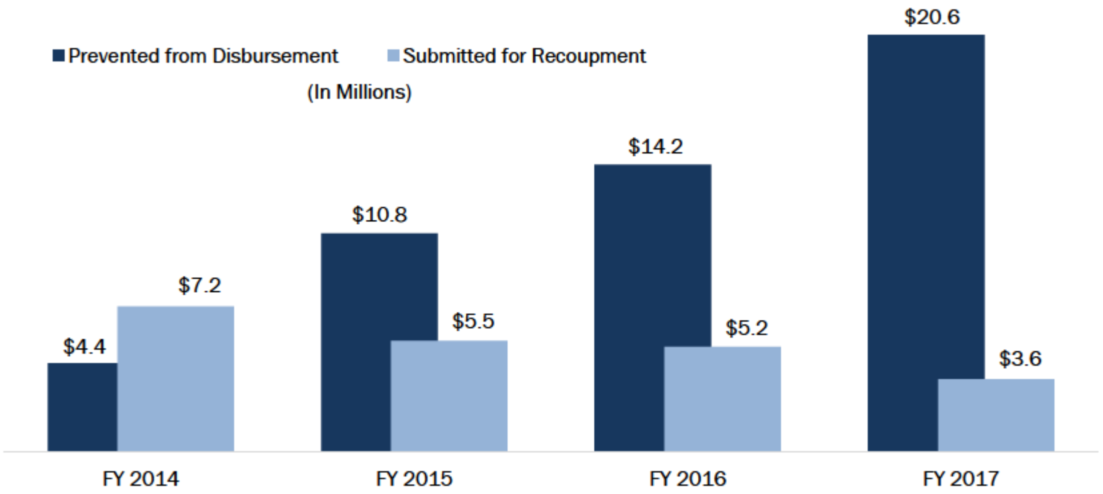


**Figure 6: Individual Assistance and Household Fraud Prevention and Recoupment**

As a continuous improvement effort, FIID identifies the datamining queries that have resulted in the highest number of fraudulent applications and uses them for every disaster. In addition, FIID provides in person, detailed fraud awareness and prevention training to all NPSC, the NFIP, the OCFO, the Federal Coordinating Officers Cadre and the FEMA Finance Center in order to provide them with information on current fraud trends as well as how to report any suspicions of fraud, waste or abuse. This initiative has opened the lines of communication to FIID and led to an increase in information sharing as well as an increase in the number of allegations of fraud referred to FIID by other components.

To help the public to report fraud, waste, and abuse, FIID added the FEMA fraud and employee misconduct email addresses as well as their 1-800 tip line telephone number to the FEMA home page, in addition to the DHS OIG fraud reporting contacts.

In response to recent disasters, FIID has prioritized Hurricanes Harvey, Irma, Maria, and Nate fraud complaints, investigations and datamining queries. FIID added fraud alerts and updates to the daily briefings (pre-shift) that is provided to all FEMA IHP intake personnel as well as information on fraud, price gouging, and how to report fraud to the National Center for Disaster Fraud (NCDF) to FEMA's webpages for Hurricane's Harvey, Irma, Maria, and Nate. FIID made contact with and is actively providing direct support to the DHS OIG in the Orlando Field Office and is prepared to provide additional resources and support to their Fraud Task Forces in Texas and Florida. FIID has also assigned a representative to the Council of Inspectors General on Integrity and Efficiency, Disaster Assistance Working Group.

## Reduce the Footprint

In FY 2015, OMB issued Management Procedures Memorandum No. 2015-01, Implementation of OMB Memorandum M-12-12 Section 3: Reduce the Footprint, dated March 25, 2015, which replaced Freeze the Footprint. During FY 2015 and FY 2016, GSA and the Department completed a predominant use reclassification exercise for the purpose of categorizing mission assets, such as land ports of entry and aviation security assets, into their proper use. This exercise resulted in a reduction in the number of DHS assets in the Department's Reduce the Footprint (RTF) baseline.

During February 2017, GSA provided the Department with their RTF report of 31.11 million square feet (SF) for FY 2016, demonstrating a net reduction of 0.1 percent from the FY 2015 RTF baseline. This actual reduction was far less than the Department's planned target due to lack of funding and reprioritization of limited funding for other projects. In addition, O&M costs increased $8 million due to incremental increases in cost across thousands of buildings assets as well as improvements in reporting of the Department's real property inventory. As the Department's reporting capability matures, future variances in reported data are possible.

Through FY 2022, DHS anticipates a 3.1 percent reduction from its RTF baseline of 31.11 million SF for office and warehouse space. Within this five-year plan, DHS projects to reduce its office space by 967 thousand SF and increase its warehouse space by 13 thousand SF for a total reduction of 954 thousand SF.

In 2017, DHS chartered a temporary Field Efficiencies Program Management Office (FE-PMO) to implement a unified cross-component planning process and identify opportunities for consolidations along common and/or similar mission functions with compatible mission support requirements, anchor locations, or future mission needs. The FE-PMO will conduct three regional studies during FY 2017 and FY 2018 and establish integrated real property mission support plans for all major metropolitan regions with a significant concentration of DHS assets and activities by FY 2022. The regional plans will focus on increased utilization of DHS assets and drive DHS office space utilization toward the DHS 150 Usable Square Feet (USF)/Full Time Equivalent (FTE) standard.

**Table 9: Reduce the Footprint Policy Baseline Comparison**

| | FY 2015 Baseline | 2016 (CY-1) | Change (FY 2015 Baseline-2016 Snapshot (CY) |
|---|---|---|---|
| Square Footage (SF in millions) | 31.14 | 31.11 | –.03 |

**Table 10: Reporting of O&M Costs – Owned and Direct Lease Buildings[2]**

| | FY 2015 Reported Cost | 2016 (CY-1) | Change (FY 2015 Baseline – FY 2016 (CY-1)) |
|---|---|---|---|
| Operation and Maintenance Costs ($ in millions) | $60 | $68 | $8 |

[2] Subject to Reduce the Footprint

## Civil Monetary Penalty Adjustment for Inflation

The Federal Civil Penalties Inflation Adjustment Act of 1990, as amended, requires agencies to make regular and consistent inflationary adjustments of civil monetary penalties to maintain their deterrent effect.

The following represents the Department's civil monetary penalties, all of which were last updated via regulation in 2017. Additional information about these penalties and the latest adjustment is available in the Federal Register, Volume 82, No. 17.

**Table 11: Civil Monetary Penalties**

| Penalty | Authority | Year Enacted | Adjusted New Penalty |
|---|---|---|---|
| CBP | | | |
| Non-compliance with arrival and departure manifest requirements for passengers, crew members, or occupants transported on commercial vessels or aircraft arriving to or departing from the United States | 8 USC 1221(g); INA Section 231(g); 8 CFR 280.53(c)(1) | 2002 | $1,333 |
| Non-compliance with landing requirements at designated ports of entry for aircraft transporting aliens | 8 USC 1224; INA Section 234; 8 CFR 280.53(c)(2) | 1990 | $3,621 |
| Violations of removal orders relating to aliens transported on vessels or aircraft under section 241(d) of the INA, or for costs associated with removal under section 241(e) of the INA | 8 USC 1253(c)(1)(A); INA Section 243(c)(1)(A); 8 CFR 280.53(c)(4) | 1996 | $3,054 |
| Failure to remove alien stowaways under section 241(d)(2) of the INA | 8 USC 1253(c)(1)(B); INA Section 243(c)(1)(B); 8 CFR 280.53(c)(5) | 1996 | $7,635 |
| Failure to report an illegal landing or desertion of alien crewmen, and for each alien not reported on arrival or departure manifest or lists required in accordance with section 251 of the USC (for each alien) | 8 USC 1281(d); INA Section 251(d); 8 CFR 280.53(c)(6) | 1990 | $362 |
| Use of alien crewmen for longshore work in violation of section 251(d) of the INA | 8 USC 1281(d); INA Section 251(d); 8 CFR 280.53(c)(6) | 1990 | $9,054 |
| Failure to control, detain, or remove alien crewmen | 8 USC 1284(a); INA Section 254(a); 8 CFR 280.53(c)(7) | 1990 | Minimum $906<br>Maximum $5,432 |
| Employment on passenger vessels of aliens afflicted with certain disabilities | 8 USC 1285; INA Section 255; 8 CFR 280.53(c)(8) | 1990 | $1,811 |
| Discharge of alien crewmen | 8 USC 1286; INA Section 256; 8 CFR 280.53(c)(9) | 1990 | Minimum $2,716<br>Maximum $5,432 |
| Bringing into the United States alien crewmen with intent to evade immigration laws | 8 USC 1287; INA Section 257; 8 CFR 280.53(c)(10) | 1990 | $18,107 |
| Failure to prevent the unauthorized landing of aliens | 8 USC § 1321(a); INA Section 271(a); 8 CFR 280.53(c)(11) | 1990 | $5,432 |
| Bringing to the United States aliens subject to denial of admission on a health-related ground | 8 USC § 1322(a); INA Section 272(a); 8 CFR 280.53(c)(12) | 1990 | $5,432 |
| Bringing to the United States aliens without required documentation | 8 USC § 1323(b); INA Section 273(b); 8 CFR 280.53(c)(13) | 1990 | $5,432 |

| Penalty | Authority | Year Enacted | Adjusted New Penalty |
|---|---|---|---|
| Improper entry | 8 USC § 1325(b)<br>INA Section 275(b); 8 CFR 280.53(c)(15) | 1996 | Minimum $76<br>Maximum $382 |
| Dealing in or using empty stamped imported liquor containers | 19 USC 469 | 1879 | $200 |
| Transporting passengers between coastwise points in the United States by a non-coastwise qualified vessel | 46 USC 55103(b); 19 CFR 4.80(b)(2 | 1898 | $300 |
| Towing a vessel between coastwise points in the United States by a non-coastwise qualified vessel | 46 USC 55111(c); 19 CFR 4.92 | 1940 | Minimum $350<br>Maximum $1100<br>plus $60 per ton |
| ICE | | | |
| Violation of Immigration and Naturalization Act (INA) sections 274C(a)(1)–(a)(4)<br>(First offense) | 8 CFR 270.3(b)(1)(ii)(A) | 1990 | Minimum $452<br>Maximum $3,621 |
| Violation of Immigration and Naturalization Act (INA) sections 274C(a)(5)–(a)(6)<br>(First offense) | 8 CFR 270.3(b)(1)(ii)(B) | 1996 | Minimum $382<br>Maximum $3,054 |
| Violation of Immigration and Naturalization Act (INA) sections 274C(a)(1)–(a)(4)<br>(Subsequent offenses) | 8 CFR 270.3(b)(1)(ii)(C) | 1990 | Minimum $3,621<br>Maximum $9,054 |
| Violation of Immigration and Naturalization Act (INA) sections 274C(a)(5)–(a)(6)<br>(Subsequent offenses) | 8 CFR 270.3(b)(1)(ii)(D) | 1996 | Minimum $3,054<br>Maximum $7,635 |
| Violation/prohibition of indemnity bonds | 8 CFR 274a.8(b) | 1986 | $2,191 |
| Knowingly hiring, recruiting, referral, or retention of unauthorized aliens (per unauthorized alien)<br>(First offense) | 8 CFR 274a.10(b)(1)(ii)(A) | 1986 | Minimum $548<br>Maximum $4,384 |
| Knowingly hiring, recruiting, referral, or retention of unauthorized aliens (per unauthorized alien)<br>(Second offense) | 8 CFR 274a.10(b)(1)(ii)(B) | 1986 | Minimum $4,384<br>Maximum $10,957 |
| Knowingly hiring, recruiting, referral, or retention of unauthorized aliens (per unauthorized alien)<br>(Subsequent offenses) | 8 CFR 274a.10(b)(1)(ii)(C) | 1986 | Minimum $6,575<br>Maximum $21,916 |
| I-9 paperwork violations | 8 CFR 274a.10(b)(2) | 1986 | Minimum $220<br>Maximum $2,191 |
| Failure to depart voluntarily | 8 USC 1229c(d); INA Section 240B(d); 8 CFR 280.53(c)(3) | 1996 | Minimum $1,527<br>Maximum $7,635 |
| Failure to depart | 8 USC 1324(d); INA Section 274D; 8 CFR 280.53(c)(14) | 1996 | $763 |
| NPPD | | | |
| Non-compliance with CFATS regulations | 6 USC 624(b)(1); 6 CFR 27.300(b)(3) | 2002 | $33,333 |
| TSA | | | |
| Certain aviation related violations by an individual or small business concern (49 CFR Ch. XII § 1503.401(c)(1)) | 49 USC 46301(a)(1), (4) | 2003 | $13,066<br>(up to a total of $65,333 per civil penalty action) |

| Penalty | Authority | Year Enacted | Adjusted New Penalty |
|---|---|---|---|
| Certain aviation related violations by any other person not operating an aircraft for the transportation of passengers or property for compensation (49 CFR Ch. XII § 1503.401(c)(2)) | 49 USC 46301(a)(1), (4) | 2003 | $13,066 (up to a total of $522,657 per civil penalty action) |
| Certain aviation related violations by a person operating an aircraft for the transportation of passengers or property for compensation (49 CFR Ch. XII § 1503.401(c)(3)) | 49 USC 46301(a)(1), (4) | 2003 | $32,666 (up to a total of $522,657 per civil penalty action) |
| Violation of any other provision of title 49 USC or of 46 USC ch. 701, or a regulation prescribed, or order issued under thereunder (49 CFR Ch. XII § 1503.401(b)) | 49 USC 114(v)(2) | 2009 | $11,182 (up to a total of $55,910 for individuals and small businesses, $447,280 for others) |
| USCG | | | |
| Saving Life and Property | 14 USC 88(c) | 2014 | $10,181 |
| Saving Life and Property (Intentional Interference with Broadcast) | 14 USC 88(e) | 2012 | $1,045 |
| Confidentiality of Medical Quality Assurance Records (first offense) | 14 USC 645(i) | 1992 | $5,114 |
| Confidentiality of Medical Quality Assurance Records (subsequent offenses) | 14 USC 645(i) | 1992 | $34,095 |
| Aquatic Nuisance Species in Waters of the United States | 16 USC 4711(g)(1) | 1996 | $38,175 |
| Obstruction of Revenue Officers by Masters of Vessels | 19 USC 70 | 1935 | $7,623 |
| Obstruction of Revenue Officers by Masters of Vessels—Minimum Penalty | 19 USC 70 | 1935 | $1,779 |
| Failure to Stop Vessel When Directed; Master, Owner, Operator or Person in Charge | 19 USC 1581(d) | 1930 | $5,000 |
| Failure to Stop Vessel When Directed; Master, Owner, Operator or Person in Charge - Minimum Penalty | 19 USC 1581(d) | 1930 | $1,000 |
| Anchorage Ground/Harbor Regulations General | 33 USC 471 | 2010 | $11,053 |
| Anchorage Ground/Harbor Regulations St. Mary's River | 33 USC 474 | 1946 | $762 |
| Bridges/Failure to Comply with Regulations | 33 USC 495(b) | 2008 | $27,904 |
| Bridges/Drawbridges | 33 USC 499(c) | 2008 | $27,904 |
| Bridges/Failure to Alter Bridge Obstructing Navigation | 33 USC 502(c) | 2008 | $27,904 |
| Bridges/Maintenance and Operation | 33 USC 533(b) | 2008 | $27,904 |
| Bridge to Bridge Communication; Master, Person in Charge or Pilot | 33 USC 1208(a) | 1971 | $2,033 |
| Bridge to Bridge Communication; Vessel | 33 USC 1208(b) | 1971 | $2,033 |
| PWSA Regulations | 33 USC 1232(a) | 1978 | $90,063 |
| Vessel Navigation: Regattas or Marine Parades; Unlicensed Person in Charge | 33 USC 1236(b) | 1990 | $9,054 |
| Vessel Navigation: Regattas or Marine Parades; Owner Onboard Vessel | 33 USC 1236(c) | 1990 | $9,054 |
| Vessel Navigation: Regattas or Marine Parades; Other Persons | 33 USC 1236(d) | 1990 | $4,527 |

| Penalty | Authority | Year Enacted | Adjusted New Penalty |
|---|---|---|---|
| Oil/Hazardous Substances: Discharges (Class I per violation) | 33 USC 1321(b)(6)(B)(i) | 1990 | $18,107 |
| Oil/Hazardous Substances: Discharges (Class I total under paragraph) | 33 USC 1321(b)(6)(B)(i) | 1990 | $45,268 |
| Oil/Hazardous Substances: Discharges (Class II per day of violation) | 33 USC 1321(b)(6)(B)(ii) | 1990 | $18,107 |
| Oil/Hazardous Substances: Discharges (Class II total under paragraph) | 33 USC 1321(b)(6)(B)(ii) | 1990 | $226,338 |
| Oil/Hazardous Substances: Discharges (per day of violation) Judicial Assessment | 33 USC 1321(b)(7)(A) | 1990 | $45,268 |
| Oil/Hazardous Substances: Discharges (per barrel of oil or unit discharged) Judicial Assessment | 33 USC 1321(b)(7)(A) | 1990 | $1,811 |
| Oil/Hazardous Substances: Failure to Carry Out Removal/Comply With Order (Judicial Assessment) | 33 USC 1321(b)(7)(B) | 1990 | $45,268 |
| Oil/Hazardous Substances: Failure to Comply with Regulation Issued Under 1321(j) (Judicial Assessment) | 33 USC 1321(b)(7)(C) | 1990 | $45,268 |
| Oil/Hazardous Substances: Discharges, Gross Negligence (per barrel of oil or unit discharged) Judicial Assessment | 33 USC 1321(b)(7)(D) | 1990 | $5,432 |
| Oil/Hazardous Substances: Discharges, Gross Negligence—Minimum Penalty (Judicial Assessment) | 33 USC 1321(b)(7)(D) | 1990 | $181,071 |
| Marine Sanitation Devices; Operating | 33 USC 1322(j) | 1972 | $7,623 |
| Marine Sanitation Devices; Sale or Manufacture | 33 USC 1322(j) | 1972 | $20,327 |
| International Navigation Rules; Operator | 33 USC 1608(a) | 1980 | $14,252 |
| International Navigation Rules; Vessel | 33 USC 1608(b) | 1980 | $14,252 |
| Pollution from Ships; General | 33 USC 1908(b)(1) | 1980 | $71,264 |
| Pollution from Ships; False Statement | 33 USC 1908(b)(2) | 1980 | $14,252 |
| Inland Navigation Rules; Operator | 33 USC 2072(a) | 1980 | $14,252 |
| Inland Navigation Rules; Vessel | 33 USC 2072(b) | 1980 | $14,252 |
| Shore Protection; General | 33 USC 2609(a) | 1988 | $50,276 |
| Shore Protection; Operating Without Permit | 33 USC 2609(b) | 1988 | $20,111 |
| Oil Pollution Liability and Compensation | 33 USC 2716a(a) | 1990 | $45,268 |
| Clean Hulls; Civil Enforcement | 33 USC 3852(a)(1)(A) | 2010 | $41,446 |
| Clean Hulls; False statements | 33 USC 3852(a)(1)(A) | 2010 | $55,263 |
| Clean Hulls; Recreational Vessel | 33 USC3852(c) | 2010 | $5,526 |
| Hazardous Substances, Releases Liability, Compensation (Class I) | 42 USC 9609(a) | 1986 | $54,789 |
| Hazardous Substances, Releases Liability, Compensation (Class II) | 42 USC 9609(b) | 1986 | $54,789 |
| Hazardous Substances, Releases Liability, Compensation (Class II subsequent offense) | 42 USC 9609(b) | 1986 | $164,367 |
| Hazardous Substances, Releases, Liability, Compensation (Judicial Assessment) | 42 USC 9609(c) | 1986 | $54,789 |
| Hazardous Substances, Releases, Liability, Compensation (Judicial Assessment subsequent offense) | 42 USC 9609(c) | 1986 | $164,367 |
| Safe Containers for International Cargo | 46 USC 80509(a) | 2006 | $5,989 |

| Penalty | Authority | Year Enacted | Adjusted New Penalty |
|---|---|---|---|
| Suspension of Passenger Service | 46 USC 70305(c) | 2006 | $59,893 |
| Vessel Inspection or Examination Fees | 46 USC 2110(e) | 1990 | $9,054 |
| Alcohol and Dangerous Drug Testing | 46 USC 2115 | 1998 | $7,370 |
| Negligent Operations: Recreational Vessels | 46 USC 2302(a) | 2002 | $6,666 |
| Negligent Operations: Other Vessels | 46 USC 2302(a) | 2002 | $33,333 |
| Operating a Vessel While Under the Influence of Alcohol or a Dangerous Drug | 46 USC 2302(c)(1) | 1998 | $7,370 |
| Vessel Reporting Requirements: Owner, Charterer, Managing Operator, or Agent | 46 USC 2306(a)(4) | 1984 | $11,478 |
| Vessel Reporting Requirements: Master | 46 USC 2306(b)(2) | 1984 | $2,296 |
| Immersion Suits | 46 USC 3102(c)(1) | 1984 | $11,478 |
| Inspection Permit | 46 USC 3302(i)(5) | 1983 | $2,394 |
| Vessel Inspection; General | 46 USC 3318(a) | 1984 | $11,478 |
| Vessel Inspection; Nautical School Vessel | 46 USC 3318(g) | 1984 | $11,478 |
| Vessel Inspection; Failure to Give Notice IAW 3304(b) | 46 USC 3318(h) | 1984 | $2,296 |
| Vessel Inspection; Failure to Give Notice IAW 3309 (c) | 46 USC 3318(i) | 1984 | $2,296 |
| Vessel Inspection; Vessel ≥ 1600 Gross Tons | 46 USC 3318(j)(1) | 1984 | $22,957 |
| Vessel Inspection; Vessel <1600 Gross Tons | 46 USC 3318(j)(1) | 1984 | $4,591 |
| Vessel Inspection; Failure to Comply with 3311(b) | 46 USC 3318(k) | 1984 | $22,957 |
| Vessel Inspection; Violation of 3318(b)-3318(f) | 46 USC 3318(l) | 1984 | $11,478 |
| List/count of Passengers | 46 USC 3502(e) | 1983 | $239 |
| Notification to Passengers | 46 USC 3504(c) | 1983 | $23,933 |
| Notification to Passengers; Sale of Tickets | 46 USC 3504(c) | 1983 | $1,196 |
| Copies of Laws on Passenger Vessels; Master | 46 USC 3506 | 1983 | $479 |
| Liquid Bulk/Dangerous Cargo | 46 USC 3718(a)(1) | 1983 | $59,834 |
| Uninspected Vessels | 46 USC 4106 | 1988 | $10,055 |
| Recreational Vessels (maximum for related series of violations) | 46 USC 4311(b)(1) | 2004 | $316,566 |
| Recreational Vessels; Violation of 4307(a) | 46 USC 4311(b)(1) | 2004 | $6,331 |
| Recreational Vessels | 46 USC 4311(c) | 1983 | $2,394 |
| Uninspected Commercial Fishing Industry Vessels | 46 USC 4507 | 1988 | $10,055 |
| Abandonment of Barges | 46 USC 4703 | 1992 | $1,704 |
| Load Lines | 46 USC 5116(a) | 1986 | $10,957 |
| Load Lines; Violation of 5112(a) | 46 USC 5116(b) | 1986 | $21,916 |
| Load Lines; Violation of 5112(b) | 46 USC 5116(c) | 1986 | $10,957 |
| Reporting Marine Casualties | 46 USC 6103(a) | 1996 | $38,175 |
| Reporting Marine Casualties; Violation of 6104 | 46 USC 6103(b) | 1988 | $10,055 |
| Manning of Inspected Vessels; Failure to Report Deficiency in Vessel Complement | 46 USC 8101(e) | 1990 | $1,811 |
| Manning of Inspected Vessels | 46 USC 8101(f) | 1990 | $18,107 |
| Manning of Inspected Vessels; Employing or Serving in Capacity not Licensed by USCG | 46 USC 8101(g) | 1990 | $18,107 |

| Penalty | Authority | Year Enacted | Adjusted New Penalty |
|---|---|---|---|
| Manning of Inspected Vessels; Freight Vessel <100 GT, Small Passenger Vessel, or Sailing School Vessel | 46 USC 8101(h) | 1983 | $2,394 |
| Watchmen on Passenger Vessels | 46 USC 8102(a) | 1983 | $2,394 |
| Citizenship Requirements | 46 USC 8103(f) | 1983 | $1,196 |
| Watches on Vessels; Violation of 8104(a) or (b) | 46 USC 8104(i) | 1990 | $18,107 |
| Watches on Vessels; Violation of 8104(c), (d), (e), or (h) | 46 USC 8104(j) | 1990 | $18,107 |
| Staff Department on Vessels | 46 USC 8302(e) | 1983 | $239 |
| Officer's Competency Certificates | 46 USC 8304(d) | 1983 | $239 |
| Coastwise Pilotage; Owner, Charterer, Managing Operator, Agent, Master or Individual in Charge | 46 USC 8502(e) | 1990 | $18,107 |
| Coastwise Pilotage; Individual | 46 USC 8502(f) | 1990 | $18,107 |
| Federal Pilots | 46 USC 8503 | 1984 | $57,391 |
| Merchant Mariners Documents | 46 USC 8701(d) | 1983 | $1,196 |
| Crew Requirements | 46 USC 8702(e) | 1990 | $18,107 |
| Small Vessel Manning | 46 USC 8906 | 1996 | $38,175 |
| Pilotage: Great Lakes; Owner, Charterer, Managing Operator, Agent, Master or Individual in Charge | 46 USC 9308(a) | 1990 | $18,107 |
| Pilotage: Great Lakes; Individual | 46 USC 9308(b) | 1990 | $18,107 |
| Pilotage: Great Lakes; Violation of 9303 | 46 USC 9308(c) | 1990 | $18,107 |
| Failure to Report Sexual Offense | 46 USC 10104(b) | 1989 | $9,623 |
| Pay Advances to Seamen | 46 USC 10314(a)(2) | 1983 | $1,196 |
| Pay Advances to Seamen; Remuneration for Employment | 46 USC 10314(b) | 1983 | $1,196 |
| Allotment to Seamen | 46 USC 10315( c ) | 1983 | $1,196 |
| Seamen Protection; General | 46 USC 10321 | 1993 | $8,296 |
| Coastwise Voyages: Advances | 46 USC 10505(a)(2) | 1993 | $8,296 |
| Coastwise Voyages: Advances; Remuneration for Employment | 46 USC 10505(b) | 1993 | $8,296 |
| Coastwise Voyages: Seamen Protection; General | 46 USC 10508(b) | 1993 | $8,296 |
| Effects of Deceased Seamen | 46 USC 10711 | 1983 | $479 |
| Complaints of Unfitness | 46 USC 10902(a)(2) | 1983 | $1,196 |
| Proceedings on Examination of Vessel | 46 USC 10903(d) | 1983 | $239 |
| Permission to Make Complaint | 46 USC 10907(b) | 1983 | $1,196 |
| Accommodations for Seamen | 46 USC 11101(f) | 1983 | $1,196 |
| Medicine Chests on Vessels | 46 USC 11102(b) | 1983 | $1,196 |
| Destitute Seamen | 46 USC 11104(b) | 1983 | $239 |
| Wages on Discharge | 46 USC 11105(c) | 1983 | $1,196 |
| Log Books; Master Failing to Maintain | 46 USC 11303(a) | 1983 | $479 |
| Log Books; Master Failing to Make Entry | 46 USC 11303(b) | 1983 | $479 |
| Log Books; Late Entry | 46 USC 11303(c) | 1983 | $359 |
| Carrying of Sheath Knives | 46 USC 11506 | 1983 | $120 |
| Documentation of Vessels | 46 USC 12151(a)(1) | 2012 | $15,675 |
| Documentation of Vessels; Activities involving mobile offshore drilling units | 46 USC 12151(a)(2) | 2012 | $26,126 |

| Penalty | Authority | Year Enacted | Adjusted New Penalty |
|---|---|---|---|
| Engaging in Fishing After Falsifying Eligibility (fine per day) | 46 USC 12151(c) | 2006 | $119,786 |
| Numbering of Undocumented Vessel; Willful violation | 46 USC 12309(a) | 1983 | $11,967 |
| Numbering of Undocumented Vessels | 46 USC 12309(b) | 1983 | $2,394 |
| Vessel Identification System | 46 USC 12507(b) | 1988 | $20,111 |
| Measurement of Vessels | 46 USC 14701 | 1986 | $43,832 |
| Measurement; False Statements | 46 USC 14702 | 1986 | $43,832 |
| Commercial Instruments and Maritime Liens | 46 USC 31309 | 1988 | $20,111 |
| Commercial Instruments and Maritime Liens; Mortgagor | 46 USC 31330(a)(2) | 1988 | $20,111 |
| Commercial Instruments and Maritime Liens; Violation of 31329 | 46 USC 31330(b)(2) | 1988 | $50,276 |
| Port Security | 46 USC 70119(a) | 2002 | $33,333 |
| Port Security; Continuing Violations | 46 USC 70119(b) | 2006 | $59,893 |
| Maritime Drug Law Enforcement; Penalties | 46 USC 70506(c) | 2010 | $5,526 |
| Hazardous Materials: Related to Vessels | 49 USC 5123(a)(1) | 2012 | $78,376 |
| Hazardous Materials: Related to Vessels; Penalty from Fatalities, Serious Injuries/ Illness or substantial Damage to Property | 49 USC 5123(a)(2) | 2012 | $182,877 |
| Hazardous Materials: Related to Vessels; Training | 49 USC 5123(a)(3) | 2012 | $471 |

## Grants Oversight & New Efficiency (GONE) Act

Enacted on January 28, 2016, the GONE Act requires each agency to submit to Congress a report on Federal grant and cooperative agreement awards which have not yet been closed and for which the period of period of performance, including any extensions, elapsed for more than two years. The following table includes DHS open grants and cooperative agreements whose period of performance ended on or before September 30, 2015.

**Table 12: Grants/Cooperative Agreements Summary Status**

($ in millions)

| CATEGORY | 2-3 Years | 3-5 Years | > 5 Years |
|---|---:|---:|---:|
| Number of Grants/Cooperative Agreements with Zero Dollar Balances | 537 | 4 | 13 |
| Number of Grants/Cooperative Agreements with Undisbursed Balances | 291 | 20 | 10 |
| Total Amount of Undisbursed Balances | $105 | $3 | $9 |

DHS awards approximately $10 billion annually in grants and cooperative agreements through eight DHS financial assistance awarding offices. The awarding offices include the Federal Emergency Management Agency (FEMA), U.S. Coast Guard, Domestic Nuclear Detection Office, Office of Health Affairs, U.S. Immigration and Customs Enforcement, National Protection & Programs Directorate, Science and Technology, and U.S. Citizenship and Immigration Services. FEMA awards ninety-eight percent of DHS grants and cooperative agreements.

DHS awarding offices use disparate grant management systems, and this has created a multitude of challenges in closing grant awards and cooperative agreements on a timely basis. Accordingly, there are inconsistent policies, procedures and processes used to award and close grants. FEMA has begun an initiative to simplify and coordinate business management and oversight approaches for its grant programs and to define grant system requirements.

Additionally, DHS is providing centralized oversight and training on grants management processes. These improved processes and an integrated systems environment will better support the close out of grants and cooperative agreements in a timely manner. Once fully implemented, DHS management officials will be able to make data-driven decisions that lead to faster action, and facilitate better outcomes for the American public.

# Other Key Regulatory Requirements

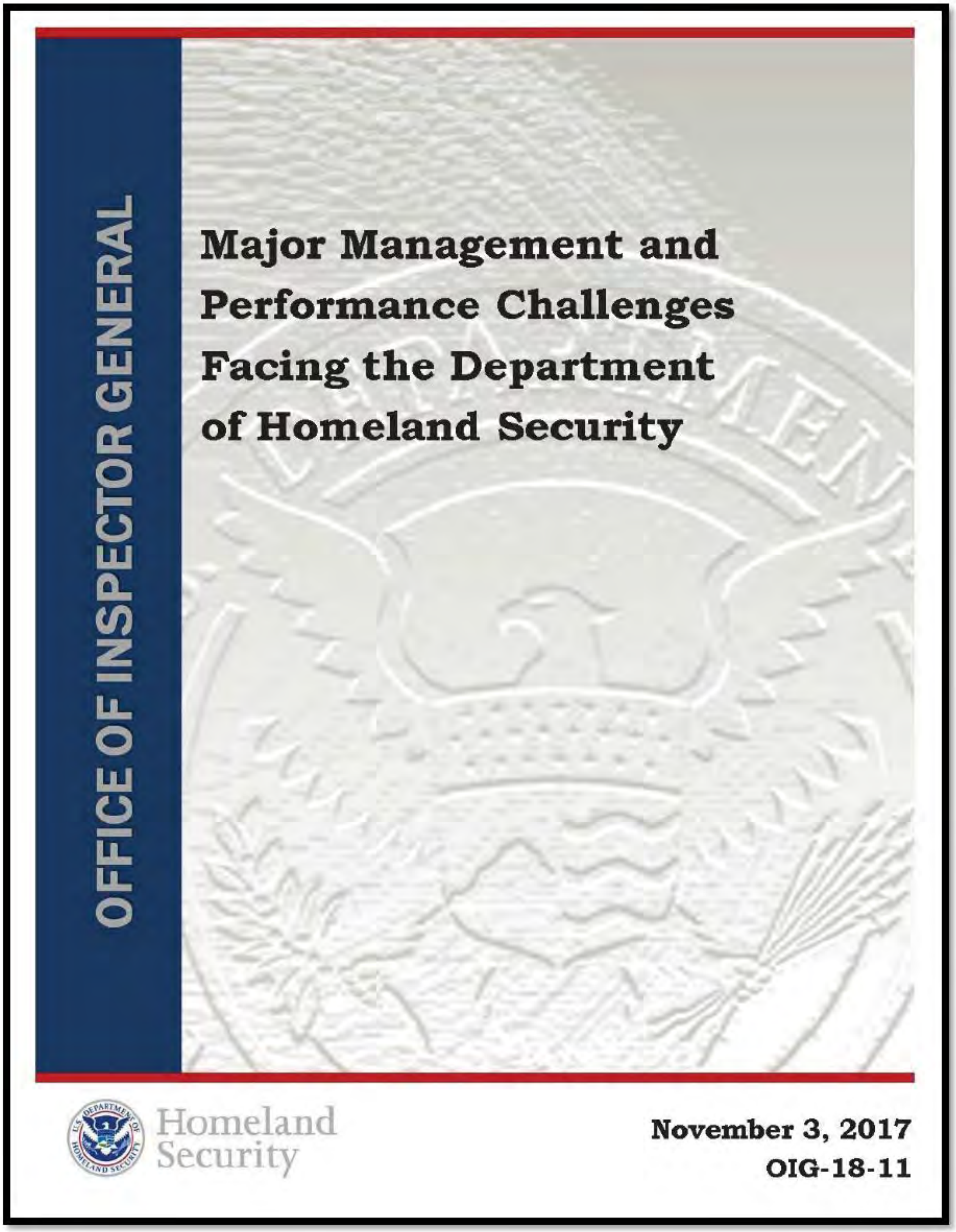
## *Prompt Payment Act*

The Prompt Payment Act requires federal agencies to make timely payments (within 30 days of receipt of invoice) to vendors for supplies and services, to pay interest penalties when payments are made after the due date, and to take cash discounts only when they are economically justified. The Department's Components submit Prompt Payment data as part of data gathered for the OMB CFO Council's Metric Tracking System (MTS). Periodic reviews are conducted by the DHS Components to identify potential problems. Interest penalties as a percentage of the dollar amount of invoices subject to the Prompt Payment Act have been measured between 0.002 percent and 0.010 percent for the period of October 2016 through September 2017, with an annual average of 0.004 percent. (Note: MTS statistics are reported with at least a six week lag).

## *Debt Collection Improvement Act*

In compliance with the Debt Collection Improvement Act of 1996 (DCIA), the Department manages its debt collection activities under the DHS DCIA regulation. The regulation is implemented under the Department's comprehensive debt collection policies that provide guidance to the Components on the administrative collection of debt; referring non-taxable debt; writing off non-taxable debt; reporting debts to consumer reporting agencies; assessing interest, penalties and administrative costs; and reporting receivables to the Treasury. The Digital Accountability and Transparency Act of 2014 was passed in May 2014 and updated DCIA requirements for referring non-taxable debt.

## *Office of Inspector General's Report on Major Management and Performance Challenges Facing the Department of Homeland Security*



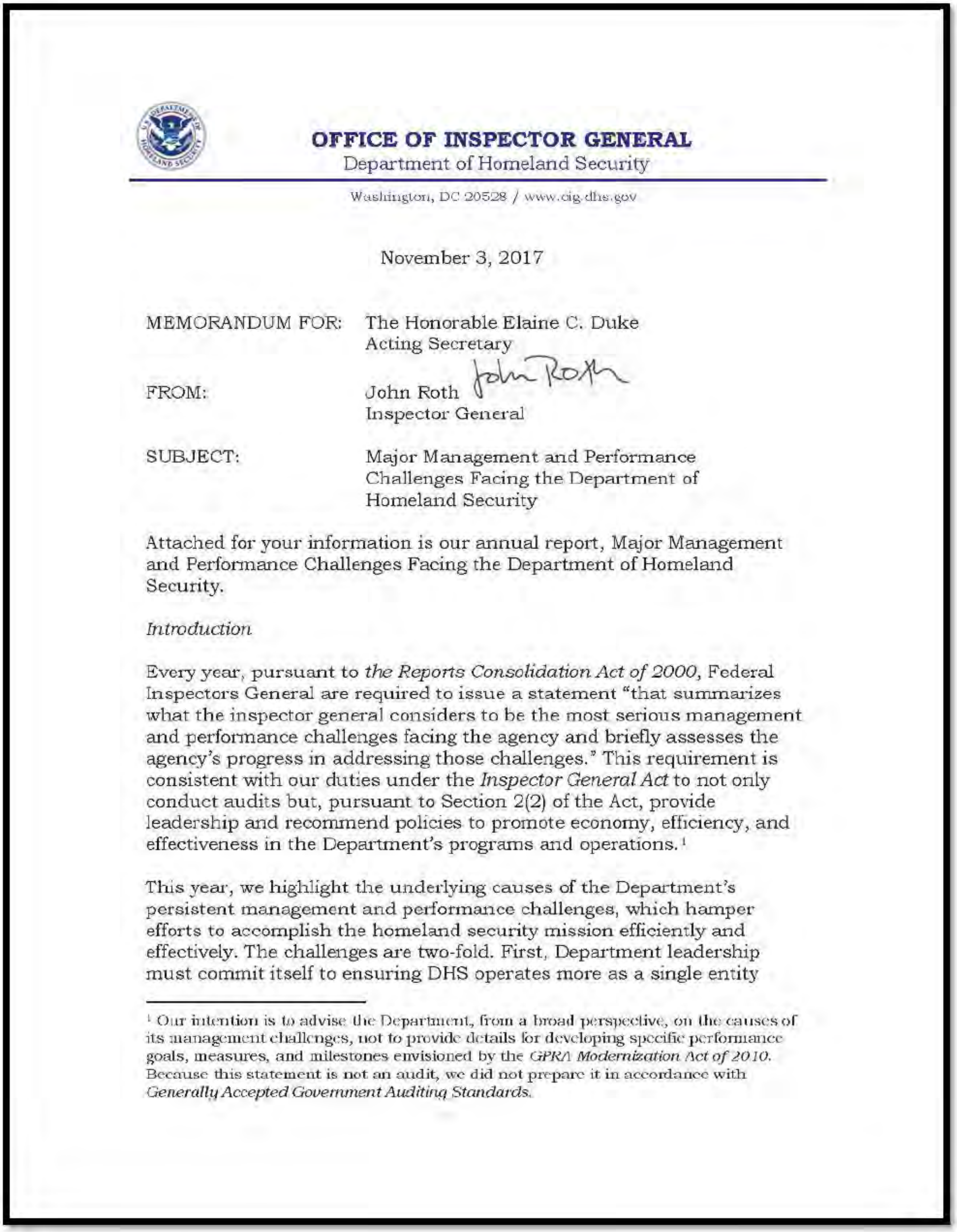
OFFICE OF INSPECTOR GENERAL

**Major Management and Performance Challenges Facing the Department of Homeland Security**

Homeland Security

**November 3, 2017**

**OIG-18-11**



**OFFICE OF INSPECTOR GENERAL**
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

November 3, 2017

MEMORANDUM FOR: The Honorable Elaine C. Duke
Acting Secretary

FROM: John Roth John Roth
Inspector General

SUBJECT: Major Management and Performance Challenges Facing the Department of Homeland Security

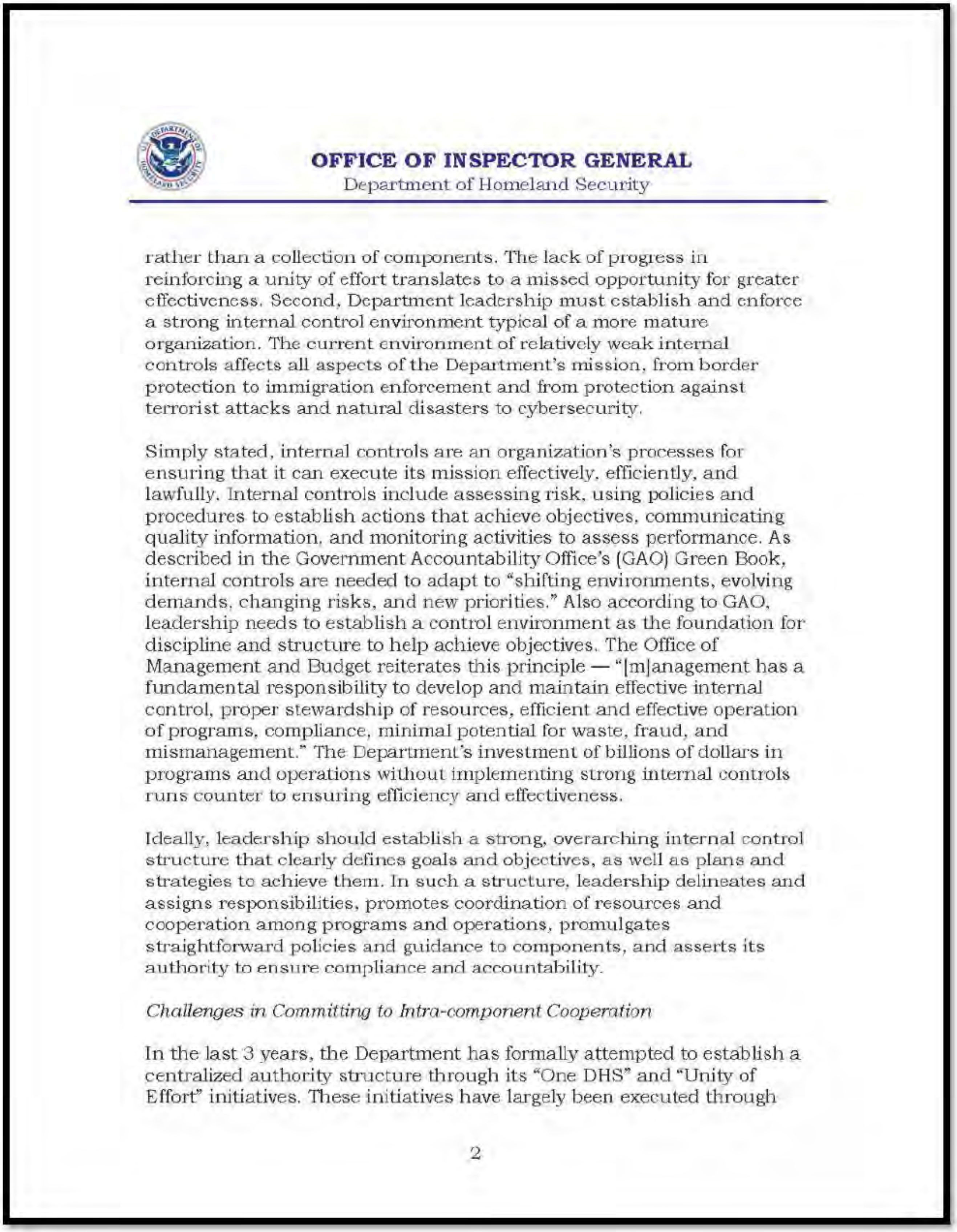
Attached for your information is our annual report, Major Management and Performance Challenges Facing the Department of Homeland Security.

*Introduction*

Every year, pursuant to *the Reports Consolidation Act of 2000*, Federal Inspectors General are required to issue a statement "that summarizes what the inspector general considers to be the most serious management and performance challenges facing the agency and briefly assesses the agency's progress in addressing those challenges." This requirement is consistent with our duties under the *Inspector General Act* to not only conduct audits but, pursuant to Section 2(2) of the Act, provide leadership and recommend policies to promote economy, efficiency, and effectiveness in the Department's programs and operations.[1]

This year, we highlight the underlying causes of the Department's persistent management and performance challenges, which hamper efforts to accomplish the homeland security mission efficiently and effectively. The challenges are two-fold. First, Department leadership must commit itself to ensuring DHS operates more as a single entity

[1] Our intention is to advise the Department, from a broad perspective, on the causes of its management challenges, not to provide details for developing specific performance goals, measures, and milestones envisioned by the *GPRA Modernization Act of 2010*. Because this statement is not an audit, we did not prepare it in accordance with *Generally Accepted Government Auditing Standards*.



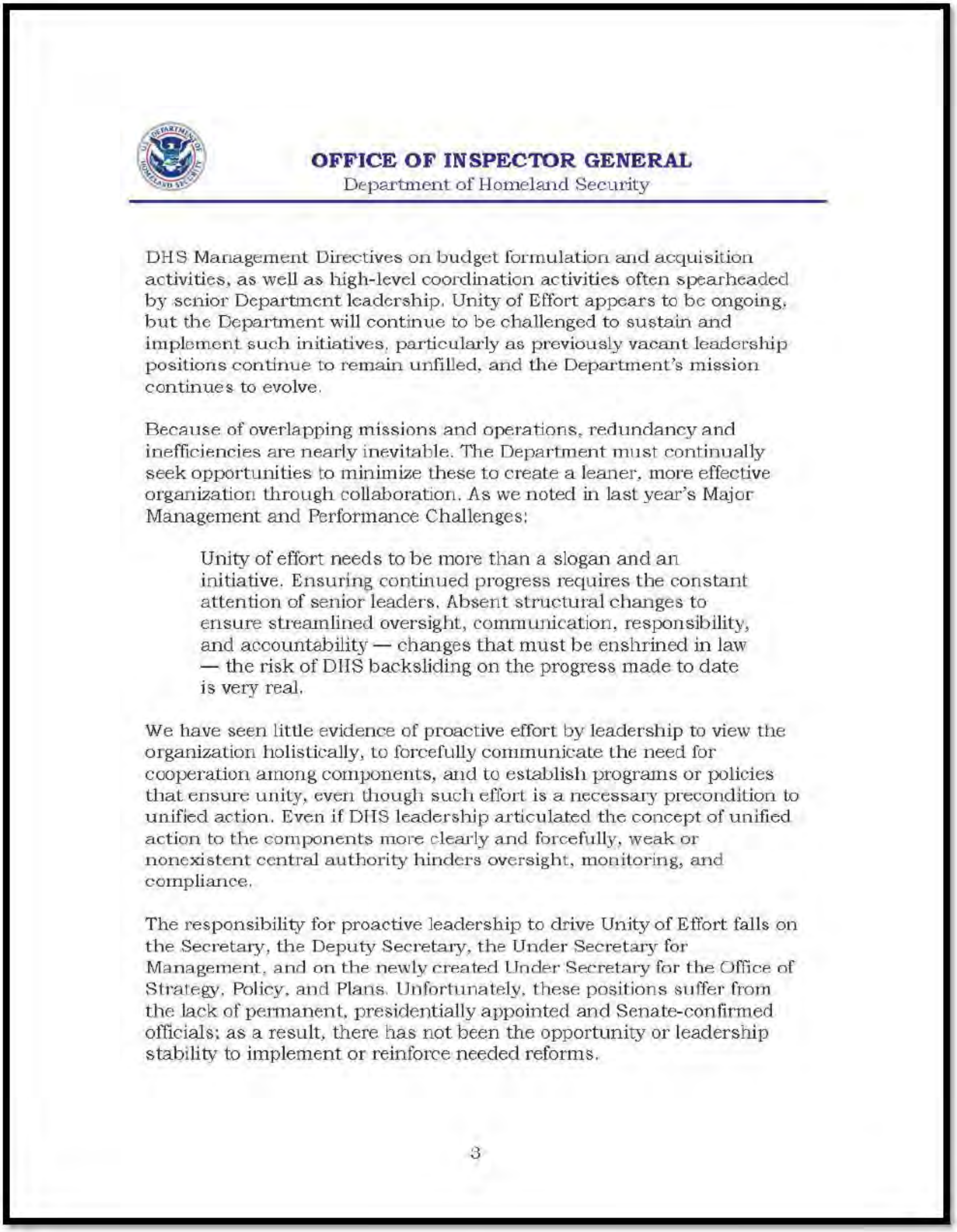
rather than a collection of components. The lack of progress in reinforcing a unity of effort translates to a missed opportunity for greater effectiveness. Second, Department leadership must establish and enforce a strong internal control environment typical of a more mature organization. The current environment of relatively weak internal controls affects all aspects of the Department's mission, from border protection to immigration enforcement and from protection against terrorist attacks and natural disasters to cybersecurity.

Simply stated, internal controls are an organization's processes for ensuring that it can execute its mission effectively, efficiently, and lawfully. Internal controls include assessing risk, using policies and procedures to establish actions that achieve objectives, communicating quality information, and monitoring activities to assess performance. As described in the Government Accountability Office's (GAO) Green Book, internal controls are needed to adapt to "shifting environments, evolving demands, changing risks, and new priorities." Also according to GAO, leadership needs to establish a control environment as the foundation for discipline and structure to help achieve objectives. The Office of Management and Budget reiterates this principle — "[m]anagement has a fundamental responsibility to develop and maintain effective internal control, proper stewardship of resources, efficient and effective operation of programs, compliance, minimal potential for waste, fraud, and mismanagement." The Department's investment of billions of dollars in programs and operations without implementing strong internal controls runs counter to ensuring efficiency and effectiveness.

Ideally, leadership should establish a strong, overarching internal control structure that clearly defines goals and objectives, as well as plans and strategies to achieve them. In such a structure, leadership delineates and assigns responsibilities, promotes coordination of resources and cooperation among programs and operations, promulgates straightforward policies and guidance to components, and asserts its authority to ensure compliance and accountability.

*Challenges in Committing to Intra-component Cooperation*

In the last 3 years, the Department has formally attempted to establish a centralized authority structure through its "One DHS" and "Unity of Effort" initiatives. These initiatives have largely been executed through



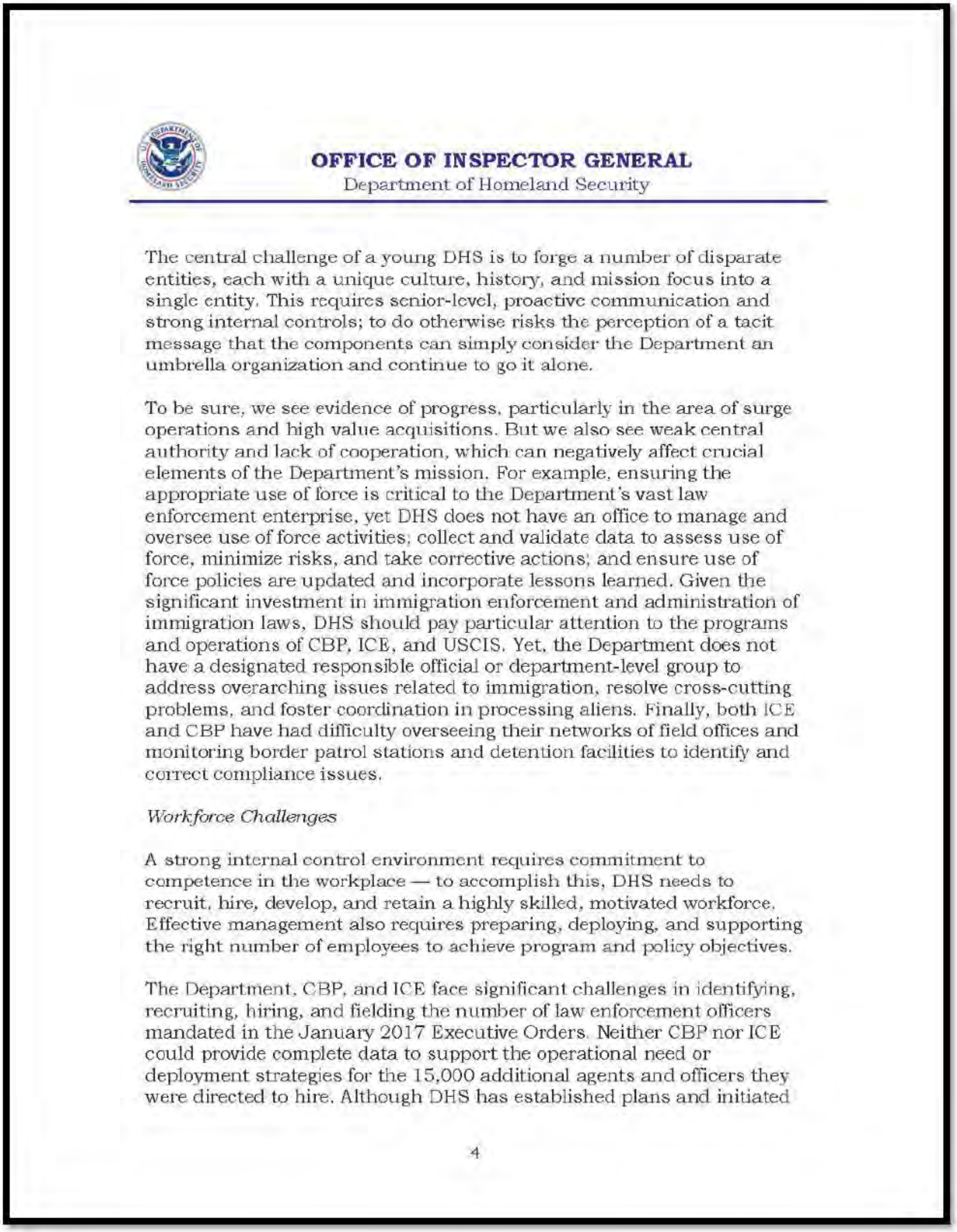
DHS Management Directives on budget formulation and acquisition activities, as well as high-level coordination activities often spearheaded by senior Department leadership. Unity of Effort appears to be ongoing, but the Department will continue to be challenged to sustain and implement such initiatives, particularly as previously vacant leadership positions continue to remain unfilled, and the Department's mission continues to evolve.

Because of overlapping missions and operations, redundancy and inefficiencies are nearly inevitable. The Department must continually seek opportunities to minimize these to create a leaner, more effective organization through collaboration. As we noted in last year's Major Management and Performance Challenges:

> Unity of effort needs to be more than a slogan and an initiative. Ensuring continued progress requires the constant attention of senior leaders. Absent structural changes to ensure streamlined oversight, communication, responsibility, and accountability — changes that must be enshrined in law — the risk of DHS backsliding on the progress made to date is very real.

We have seen little evidence of proactive effort by leadership to view the organization holistically, to forcefully communicate the need for cooperation among components, and to establish programs or policies that ensure unity, even though such effort is a necessary precondition to unified action. Even if DHS leadership articulated the concept of unified action to the components more clearly and forcefully, weak or nonexistent central authority hinders oversight, monitoring, and compliance.

The responsibility for proactive leadership to drive Unity of Effort falls on the Secretary, the Deputy Secretary, the Under Secretary for Management, and on the newly created Under Secretary for the Office of Strategy, Policy, and Plans. Unfortunately, these positions suffer from the lack of permanent, presidentially appointed and Senate-confirmed officials; as a result, there has not been the opportunity or leadership stability to implement or reinforce needed reforms.



**OFFICE OF INSPECTOR GENERAL**
Department of Homeland Security

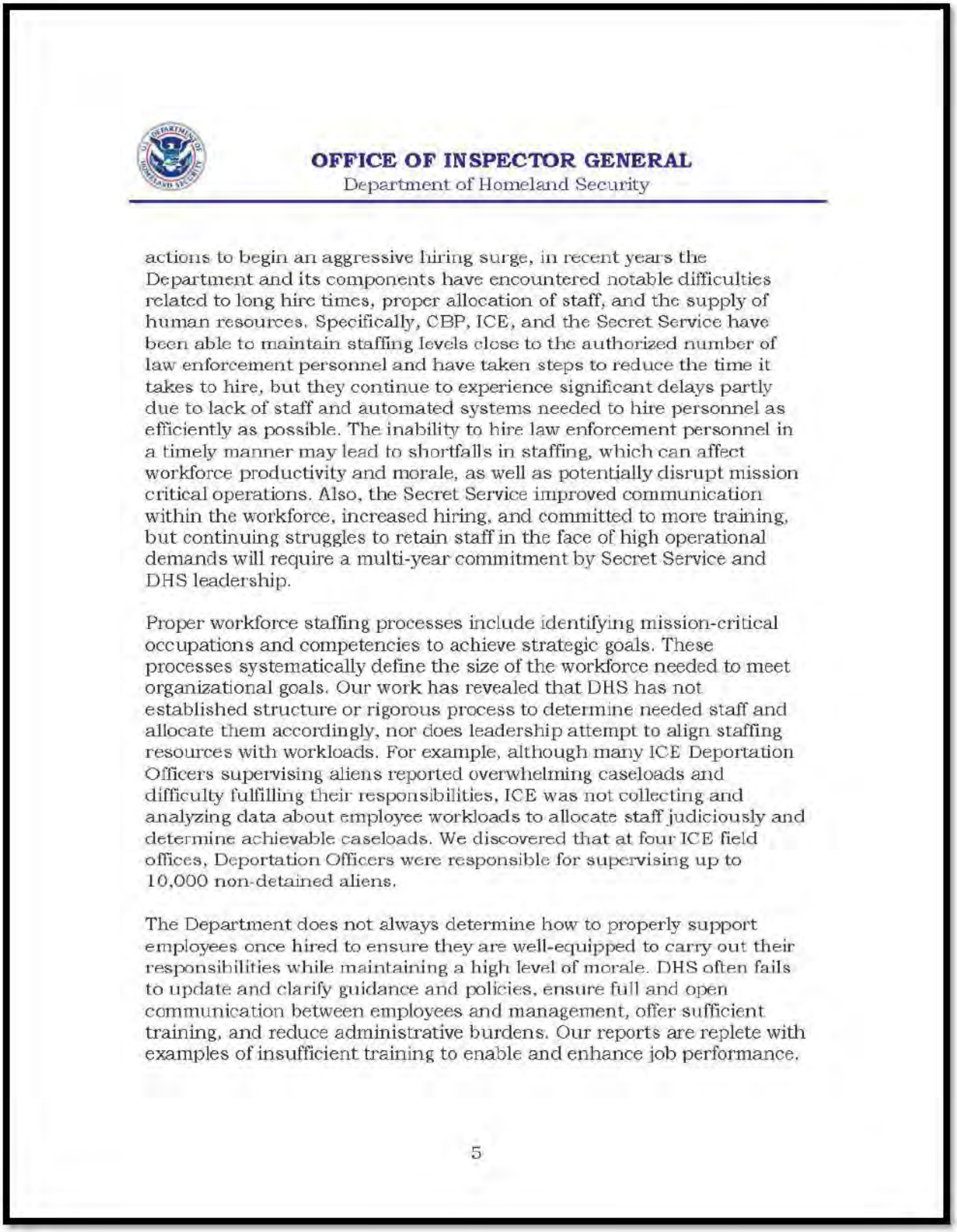
The central challenge of a young DHS is to forge a number of disparate entities, each with a unique culture, history, and mission focus into a single entity. This requires senior-level, proactive communication and strong internal controls; to do otherwise risks the perception of a tacit message that the components can simply consider the Department an umbrella organization and continue to go it alone.

To be sure, we see evidence of progress, particularly in the area of surge operations and high value acquisitions. But we also see weak central authority and lack of cooperation, which can negatively affect crucial elements of the Department's mission. For example, ensuring the appropriate use of force is critical to the Department's vast law enforcement enterprise, yet DHS does not have an office to manage and oversee use of force activities; collect and validate data to assess use of force, minimize risks, and take corrective actions; and ensure use of force policies are updated and incorporate lessons learned. Given the significant investment in immigration enforcement and administration of immigration laws, DHS should pay particular attention to the programs and operations of CBP, ICE, and USCIS. Yet, the Department does not have a designated responsible official or department-level group to address overarching issues related to immigration, resolve cross-cutting problems, and foster coordination in processing aliens. Finally, both ICE and CBP have had difficulty overseeing their networks of field offices and monitoring border patrol stations and detention facilities to identify and correct compliance issues.

*Workforce Challenges*

A strong internal control environment requires commitment to competence in the workplace — to accomplish this, DHS needs to recruit, hire, develop, and retain a highly skilled, motivated workforce. Effective management also requires preparing, deploying, and supporting the right number of employees to achieve program and policy objectives.

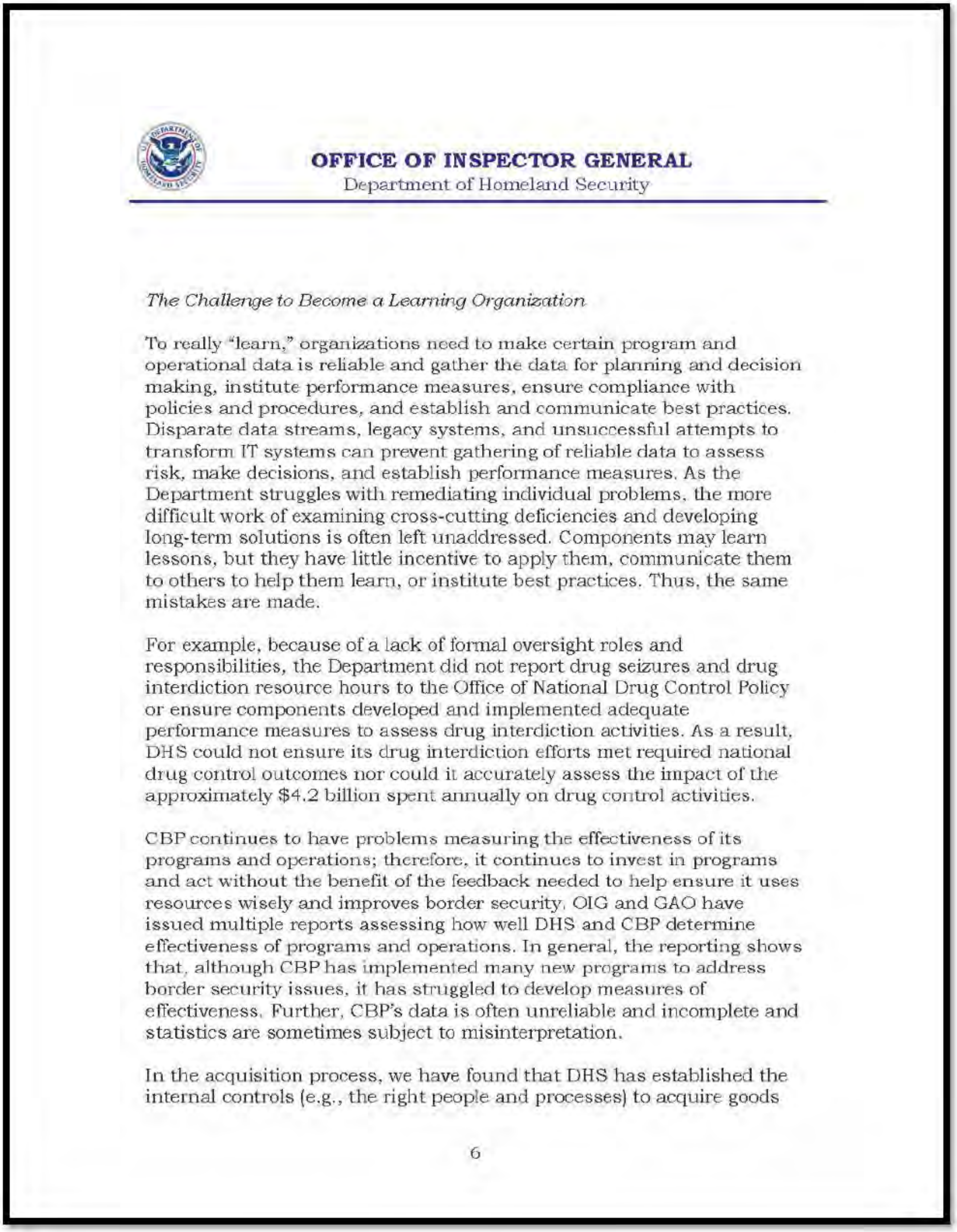
The Department, CBP, and ICE face significant challenges in identifying, recruiting, hiring, and fielding the number of law enforcement officers mandated in the January 2017 Executive Orders. Neither CBP nor ICE could provide complete data to support the operational need or deployment strategies for the 15,000 additional agents and officers they were directed to hire. Although DHS has established plans and initiated



actions to begin an aggressive hiring surge, in recent years the Department and its components have encountered notable difficulties related to long hire times, proper allocation of staff, and the supply of human resources. Specifically, CBP, ICE, and the Secret Service have been able to maintain staffing levels close to the authorized number of law enforcement personnel and have taken steps to reduce the time it takes to hire, but they continue to experience significant delays partly due to lack of staff and automated systems needed to hire personnel as efficiently as possible. The inability to hire law enforcement personnel in a timely manner may lead to shortfalls in staffing, which can affect workforce productivity and morale, as well as potentially disrupt mission critical operations. Also, the Secret Service improved communication within the workforce, increased hiring, and committed to more training, but continuing struggles to retain staff in the face of high operational demands will require a multi-year commitment by Secret Service and DHS leadership.

Proper workforce staffing processes include identifying mission-critical occupations and competencies to achieve strategic goals. These processes systematically define the size of the workforce needed to meet organizational goals. Our work has revealed that DHS has not established structure or rigorous process to determine needed staff and allocate them accordingly, nor does leadership attempt to align staffing resources with workloads. For example, although many ICE Deportation Officers supervising aliens reported overwhelming caseloads and difficulty fulfilling their responsibilities, ICE was not collecting and analyzing data about employee workloads to allocate staff judiciously and determine achievable caseloads. We discovered that at four ICE field offices, Deportation Officers were responsible for supervising up to 10,000 non-detained aliens.

The Department does not always determine how to properly support employees once hired to ensure they are well-equipped to carry out their responsibilities while maintaining a high level of morale. DHS often fails to update and clarify guidance and policies, ensure full and open communication between employees and management, offer sufficient training, and reduce administrative burdens. Our reports are replete with examples of insufficient training to enable and enhance job performance.



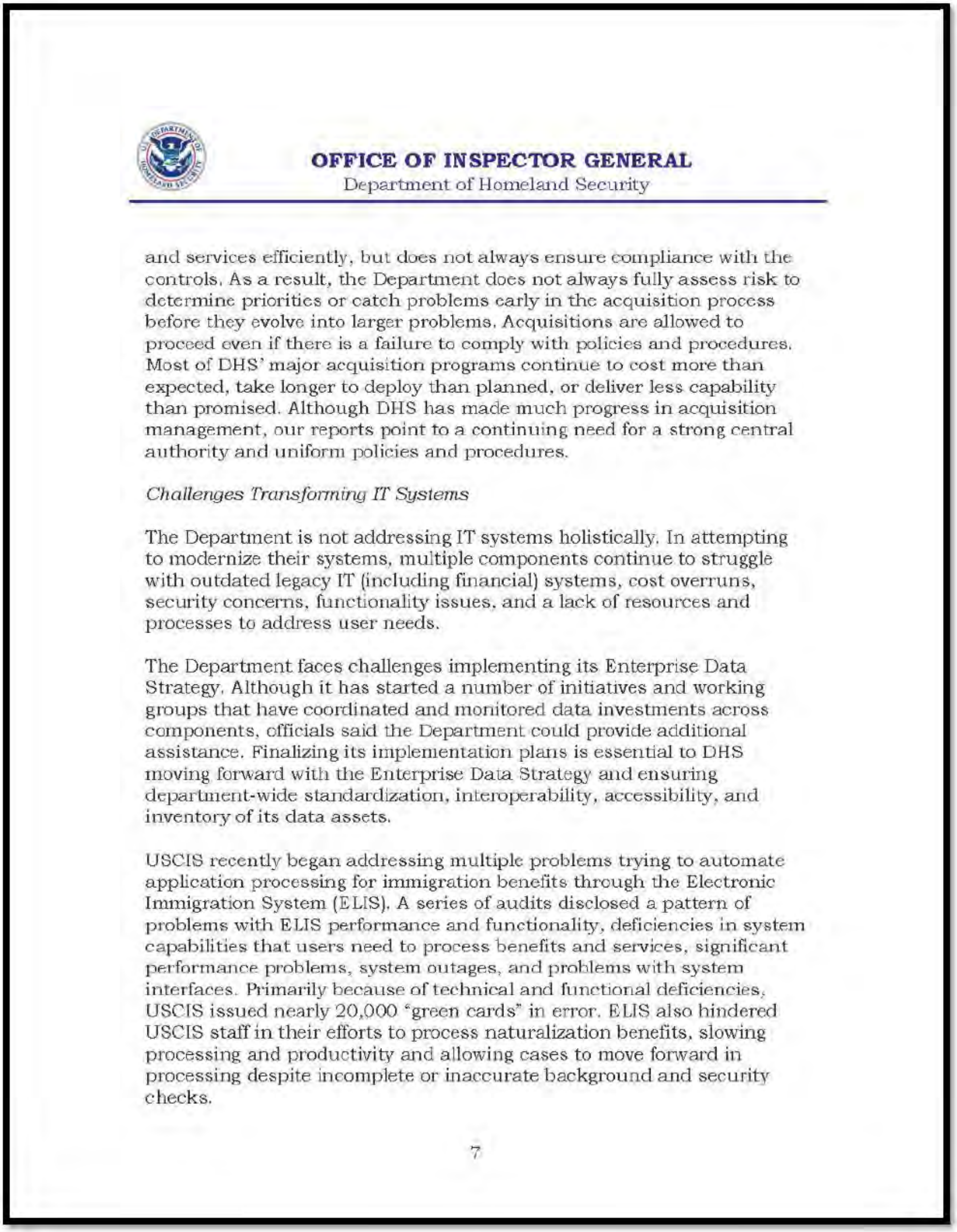
*The Challenge to Become a Learning Organization*

To really "learn," organizations need to make certain program and operational data is reliable and gather the data for planning and decision making, institute performance measures, ensure compliance with policies and procedures, and establish and communicate best practices. Disparate data streams, legacy systems, and unsuccessful attempts to transform IT systems can prevent gathering of reliable data to assess risk, make decisions, and establish performance measures. As the Department struggles with remediating individual problems, the more difficult work of examining cross-cutting deficiencies and developing long-term solutions is often left unaddressed. Components may learn lessons, but they have little incentive to apply them, communicate them to others to help them learn, or institute best practices. Thus, the same mistakes are made.

For example, because of a lack of formal oversight roles and responsibilities, the Department did not report drug seizures and drug interdiction resource hours to the Office of National Drug Control Policy or ensure components developed and implemented adequate performance measures to assess drug interdiction activities. As a result, DHS could not ensure its drug interdiction efforts met required national drug control outcomes nor could it accurately assess the impact of the approximately $4.2 billion spent annually on drug control activities.

CBP continues to have problems measuring the effectiveness of its programs and operations; therefore, it continues to invest in programs and act without the benefit of the feedback needed to help ensure it uses resources wisely and improves border security. OIG and GAO have issued multiple reports assessing how well DHS and CBP determine effectiveness of programs and operations. In general, the reporting shows that, although CBP has implemented many new programs to address border security issues, it has struggled to develop measures of effectiveness. Further, CBP's data is often unreliable and incomplete and statistics are sometimes subject to misinterpretation.

In the acquisition process, we have found that DHS has established the internal controls (e.g., the right people and processes) to acquire goods



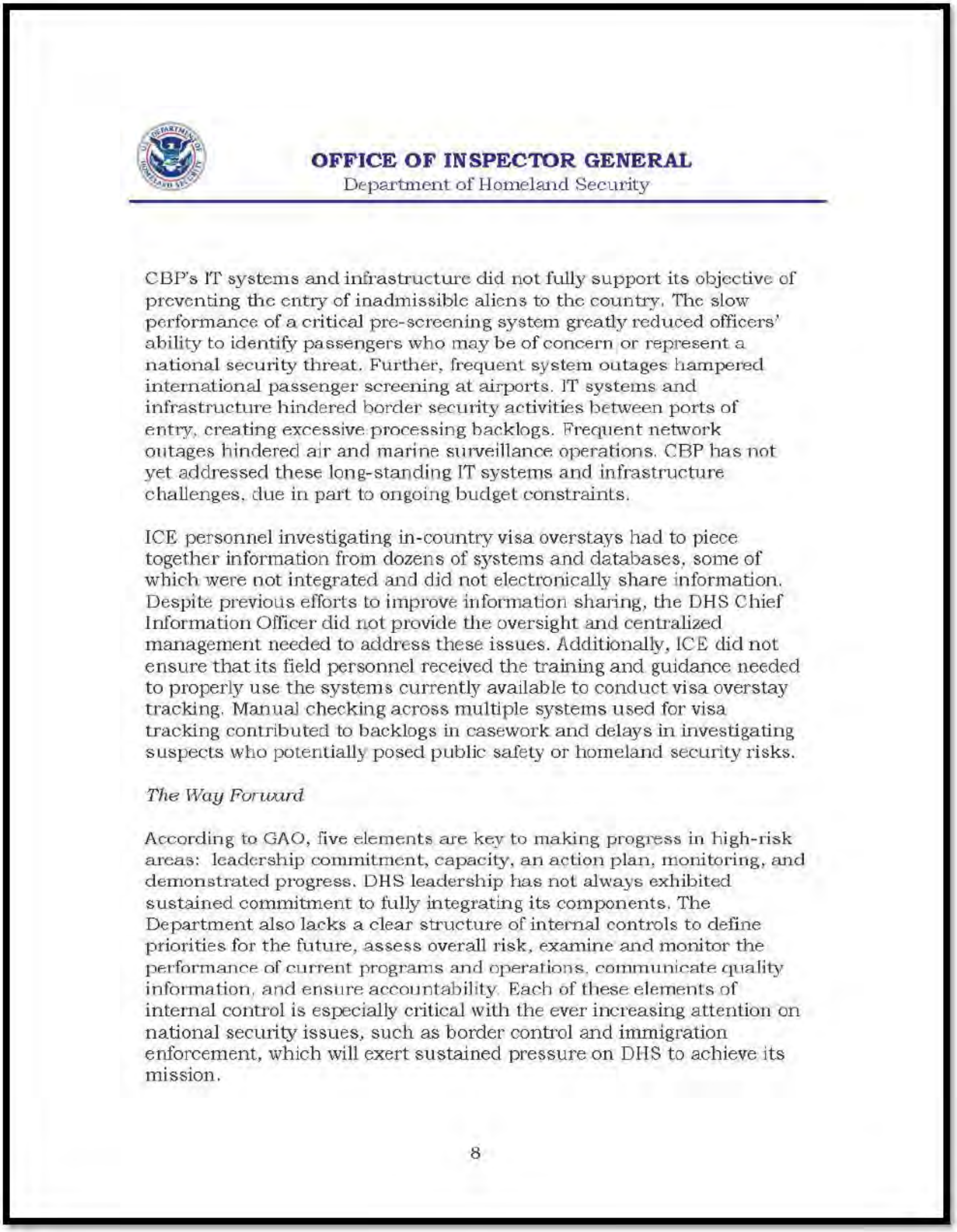
and services efficiently, but does not always ensure compliance with the controls. As a result, the Department does not always fully assess risk to determine priorities or catch problems early in the acquisition process before they evolve into larger problems. Acquisitions are allowed to proceed even if there is a failure to comply with policies and procedures. Most of DHS' major acquisition programs continue to cost more than expected, take longer to deploy than planned, or deliver less capability than promised. Although DHS has made much progress in acquisition management, our reports point to a continuing need for a strong central authority and uniform policies and procedures.

*Challenges Transforming IT Systems*

The Department is not addressing IT systems holistically. In attempting to modernize their systems, multiple components continue to struggle with outdated legacy IT (including financial) systems, cost overruns, security concerns, functionality issues, and a lack of resources and processes to address user needs.

The Department faces challenges implementing its Enterprise Data Strategy. Although it has started a number of initiatives and working groups that have coordinated and monitored data investments across components, officials said the Department could provide additional assistance. Finalizing its implementation plans is essential to DHS moving forward with the Enterprise Data Strategy and ensuring department-wide standardization, interoperability, accessibility, and inventory of its data assets.

USCIS recently began addressing multiple problems trying to automate application processing for immigration benefits through the Electronic Immigration System (ELIS). A series of audits disclosed a pattern of problems with ELIS performance and functionality, deficiencies in system capabilities that users need to process benefits and services, significant performance problems, system outages, and problems with system interfaces. Primarily because of technical and functional deficiencies, USCIS issued nearly 20,000 "green cards" in error. ELIS also hindered USCIS staff in their efforts to process naturalization benefits, slowing processing and productivity and allowing cases to move forward in processing despite incomplete or inaccurate background and security checks.

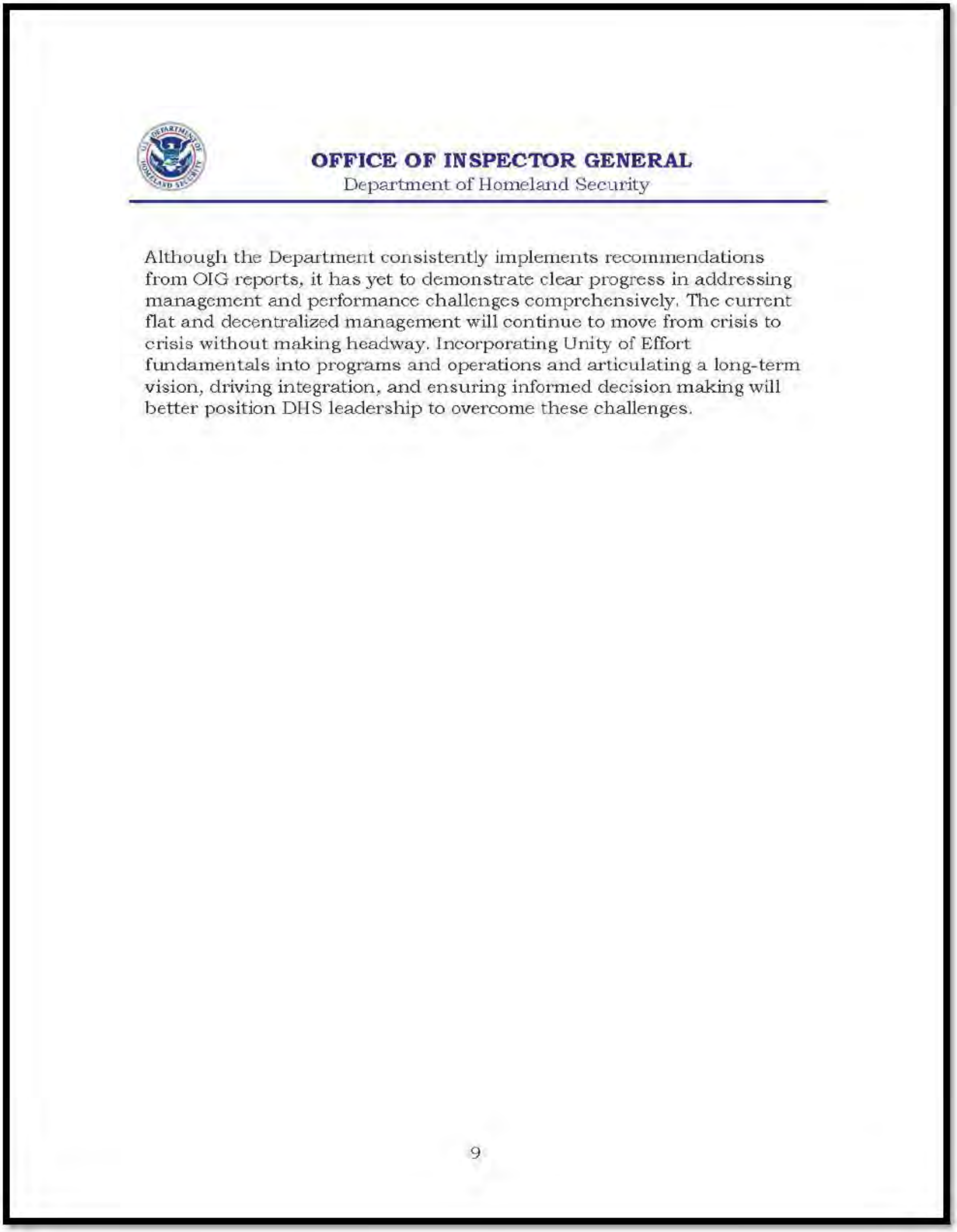


CBP's IT systems and infrastructure did not fully support its objective of preventing the entry of inadmissible aliens to the country. The slow performance of a critical pre-screening system greatly reduced officers' ability to identify passengers who may be of concern or represent a national security threat. Further, frequent system outages hampered international passenger screening at airports. IT systems and infrastructure hindered border security activities between ports of entry, creating excessive processing backlogs. Frequent network outages hindered air and marine surveillance operations. CBP has not yet addressed these long-standing IT systems and infrastructure challenges, due in part to ongoing budget constraints.

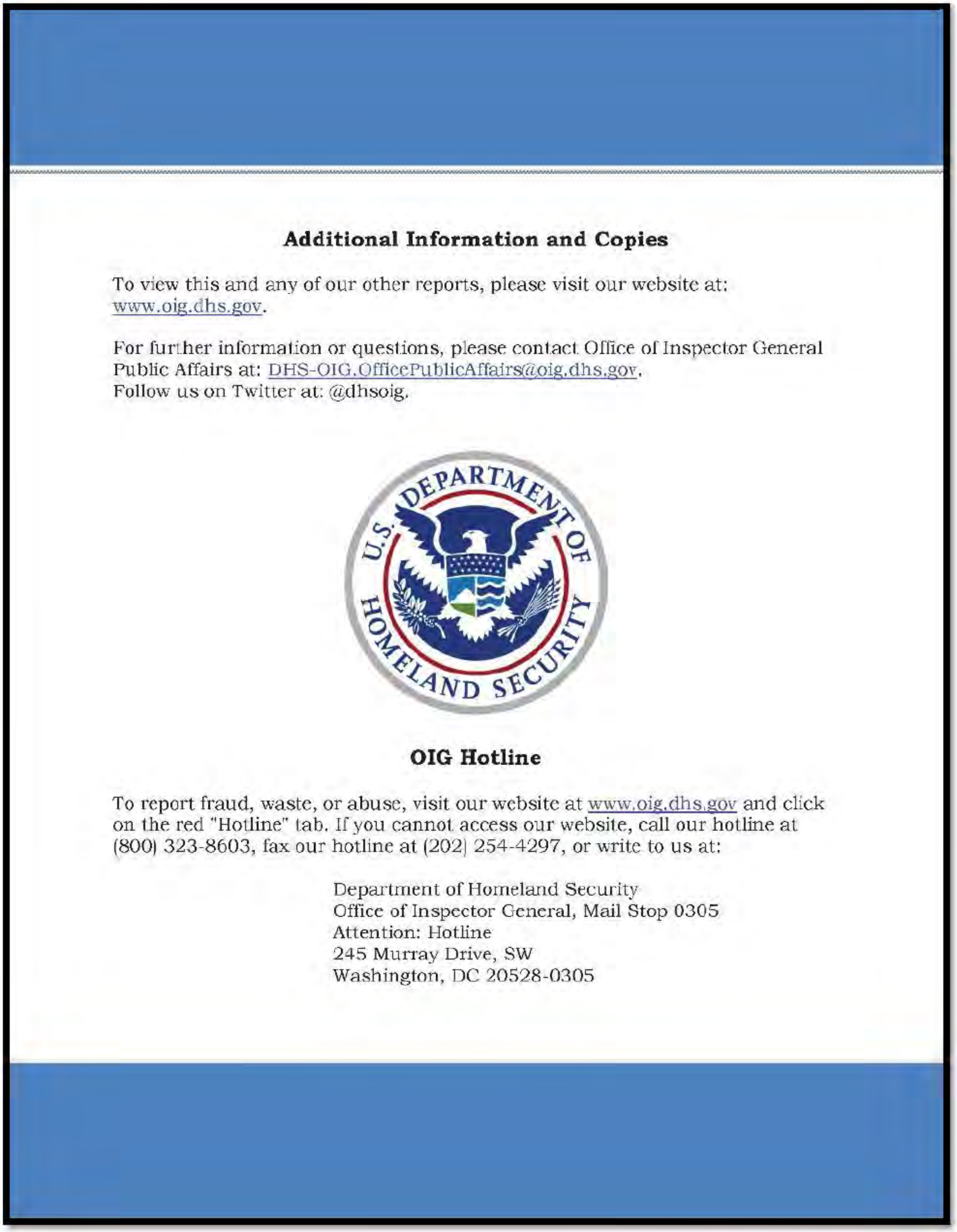
ICE personnel investigating in-country visa overstays had to piece together information from dozens of systems and databases, some of which were not integrated and did not electronically share information. Despite previous efforts to improve information sharing, the DHS Chief Information Officer did not provide the oversight and centralized management needed to address these issues. Additionally, ICE did not ensure that its field personnel received the training and guidance needed to properly use the systems currently available to conduct visa overstay tracking. Manual checking across multiple systems used for visa tracking contributed to backlogs in casework and delays in investigating suspects who potentially posed public safety or homeland security risks.

*The Way Forward*

According to GAO, five elements are key to making progress in high-risk areas: leadership commitment, capacity, an action plan, monitoring, and demonstrated progress. DHS leadership has not always exhibited sustained commitment to fully integrating its components. The Department also lacks a clear structure of internal controls to define priorities for the future, assess overall risk, examine and monitor the performance of current programs and operations, communicate quality information, and ensure accountability. Each of these elements of internal control is especially critical with the ever increasing attention on national security issues, such as border control and immigration enforcement, which will exert sustained pressure on DHS to achieve its mission.



Although the Department consistently implements recommendations from OIG reports, it has yet to demonstrate clear progress in addressing management and performance challenges comprehensively. The current flat and decentralized management will continue to move from crisis to crisis without making headway. Incorporating Unity of Effort fundamentals into programs and operations and articulating a long-term vision, driving integration, and ensuring informed decision making will better position DHS leadership to overcome these challenges.



## Additional Information and Copies

To view this and any of our other reports, please visit our website at: www.oig.dhs.gov.

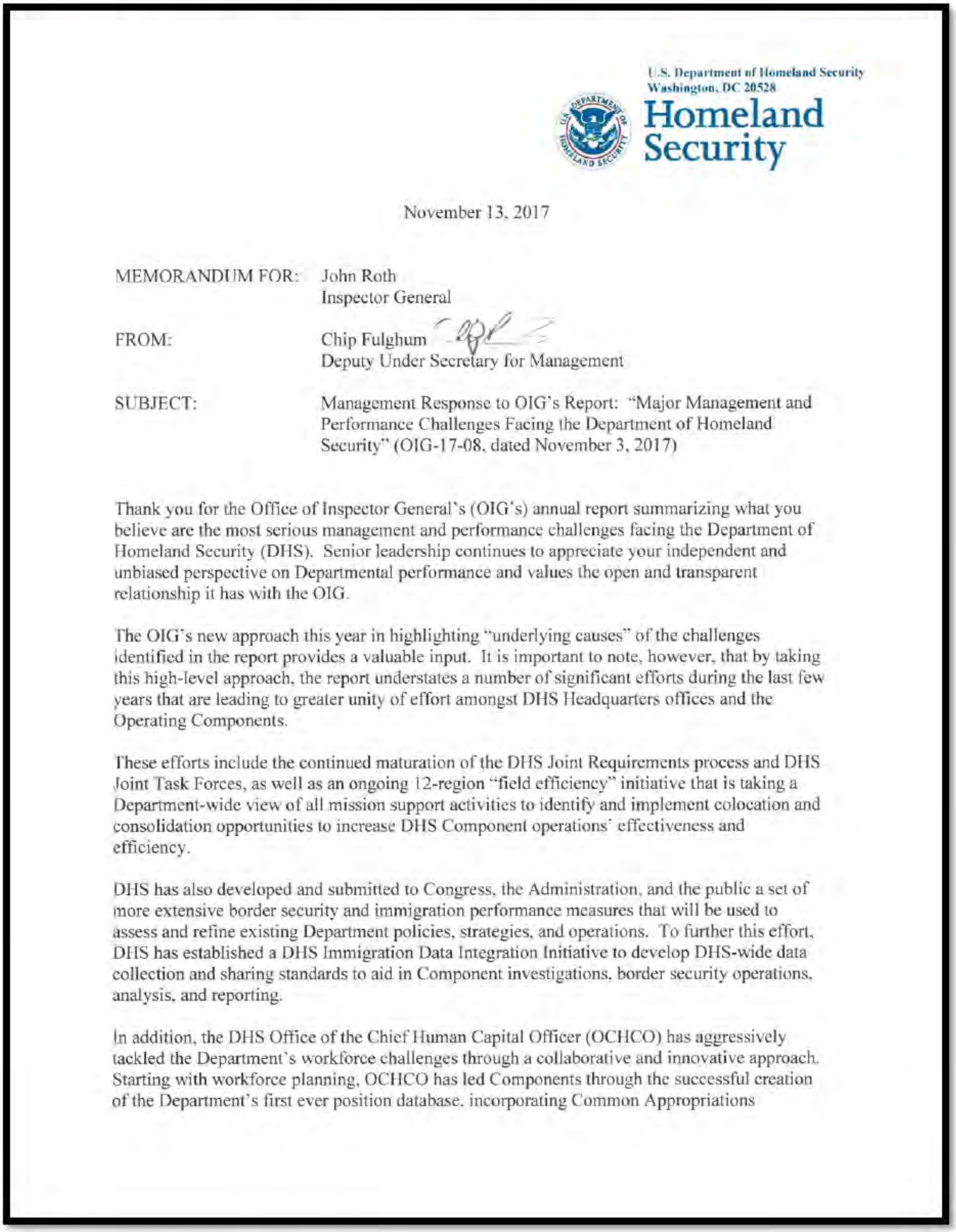
For further information or questions, please contact Office of Inspector General Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov.
Follow us on Twitter at: @dhsoig.

## OIG Hotline

To report fraud, waste, or abuse, visit our website at www.oig.dhs.gov and click on the red "Hotline" tab. If you cannot access our website, call our hotline at (800) 323-8603, fax our hotline at (202) 254-4297, or write to us at:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Hotline
245 Murray Drive, SW
Washington, DC 20528-0305

## *Management's Response to OIG's Report on Major Management and Performance Challenges Facing the Department of Homeland Security*



U.S. Department of Homeland Security
Washington, DC 20528
Homeland Security

November 13, 2017

MEMORANDUM FOR: John Roth
Inspector General

FROM: Chip Fulghum
Deputy Under Secretary for Management

SUBJECT: Management Response to OIG's Report: "Major Management and Performance Challenges Facing the Department of Homeland Security" (OIG-17-08, dated November 3, 2017)

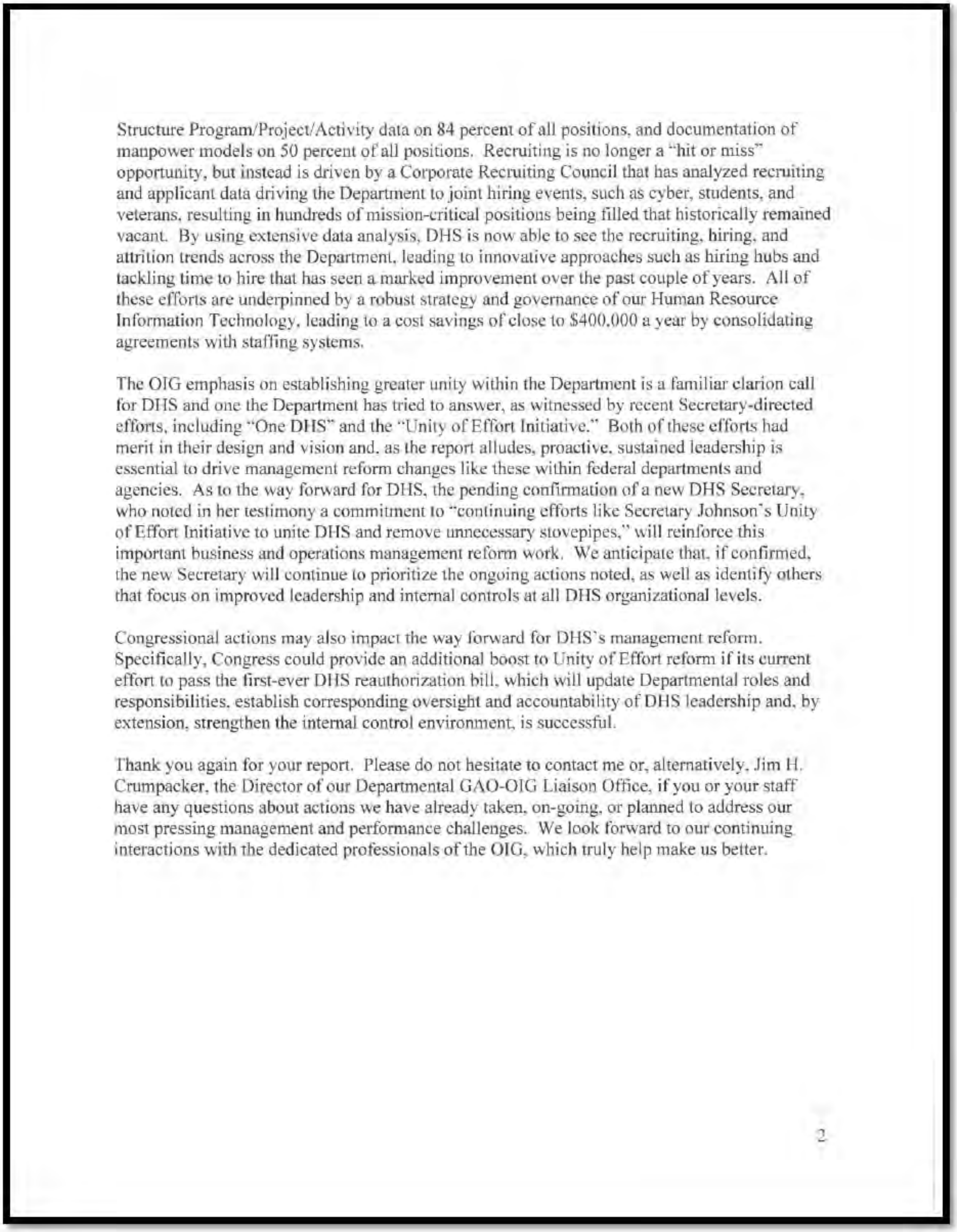
Thank you for the Office of Inspector General's (OIG's) annual report summarizing what you believe are the most serious management and performance challenges facing the Department of Homeland Security (DHS). Senior leadership continues to appreciate your independent and unbiased perspective on Departmental performance and values the open and transparent relationship it has with the OIG.

The OIG's new approach this year in highlighting "underlying causes" of the challenges identified in the report provides a valuable input. It is important to note, however, that by taking this high-level approach, the report understates a number of significant efforts during the last few years that are leading to greater unity of effort amongst DHS Headquarters offices and the Operating Components.

These efforts include the continued maturation of the DHS Joint Requirements process and DHS Joint Task Forces, as well as an ongoing 12-region "field efficiency" initiative that is taking a Department-wide view of all mission support activities to identify and implement colocation and consolidation opportunities to increase DHS Component operations' effectiveness and efficiency.

DHS has also developed and submitted to Congress, the Administration, and the public a set of more extensive border security and immigration performance measures that will be used to assess and refine existing Department policies, strategies, and operations. To further this effort, DHS has established a DHS Immigration Data Integration Initiative to develop DHS-wide data collection and sharing standards to aid in Component investigations, border security operations, analysis, and reporting.

In addition, the DHS Office of the Chief Human Capital Officer (OCHCO) has aggressively tackled the Department's workforce challenges through a collaborative and innovative approach. Starting with workforce planning, OCHCO has led Components through the successful creation of the Department's first ever position database, incorporating Common Appropriations



Structure Program/Project/Activity data on 84 percent of all positions, and documentation of manpower models on 50 percent of all positions. Recruiting is no longer a "hit or miss" opportunity, but instead is driven by a Corporate Recruiting Council that has analyzed recruiting and applicant data driving the Department to joint hiring events, such as cyber, students, and veterans, resulting in hundreds of mission-critical positions being filled that historically remained vacant. By using extensive data analysis, DHS is now able to see the recruiting, hiring, and attrition trends across the Department, leading to innovative approaches such as hiring hubs and tackling time to hire that has seen a marked improvement over the past couple of years. All of these efforts are underpinned by a robust strategy and governance of our Human Resource Information Technology, leading to a cost savings of close to $400,000 a year by consolidating agreements with staffing systems.

The OIG emphasis on establishing greater unity within the Department is a familiar clarion call for DHS and one the Department has tried to answer, as witnessed by recent Secretary-directed efforts, including "One DHS" and the "Unity of Effort Initiative." Both of these efforts had merit in their design and vision and, as the report alludes, proactive, sustained leadership is essential to drive management reform changes like these within federal departments and agencies. As to the way forward for DHS, the pending confirmation of a new DHS Secretary, who noted in her testimony a commitment to "continuing efforts like Secretary Johnson's Unity of Effort Initiative to unite DHS and remove unnecessary stovepipes," will reinforce this important business and operations management reform work. We anticipate that, if confirmed, the new Secretary will continue to prioritize the ongoing actions noted, as well as identify others that focus on improved leadership and internal controls at all DHS organizational levels.

Congressional actions may also impact the way forward for DHS's management reform. Specifically, Congress could provide an additional boost to Unity of Effort reform if its current effort to pass the first-ever DHS reauthorization bill, which will update Departmental roles and responsibilities, establish corresponding oversight and accountability of DHS leadership and, by extension, strengthen the internal control environment, is successful.

Thank you again for your report. Please do not hesitate to contact me or, alternatively, Jim H. Crumpacker, the Director of our Departmental GAO-OIG Liaison Office, if you or your staff have any questions about actions we have already taken, on-going, or planned to address our most pressing management and performance challenges. We look forward to our continuing interactions with the dedicated professionals of the OIG, which truly help make us better.

# Acronym List

# Acronyms

AFG – Assistance to Firefighters Grants
AFR – Agency Financial Report
AUO – Administratively Uncontrollable Overtime
CBP – U.S. Customs and Border Protection
CDL – Community Disaster Loans
CDM – Continuous Diagnostics and Mitigation
CDP – Center for Domestic Preparedness
CEAR – Certificate of Excellence in Accountability Reporting
CFATS – Chemical Facility Anti–Terrorism Standards
CFO – Chief Financial Officer
CFR – Code of Federal Regulations
CIO – Chief Information Officer
COBRA – Consolidated Omnibus Budget Reconciliation Act of 1985
COTS – Commercial Off–the–Shelf
CSATS – Chemical Security Assessment Tool
CSRS – Civil Service Retirement System
CY – Current Year
DADLP – Disaster Assistance Direct Loan Program
DC – District of Columbia
DCIA – Debt Collection Improvement Act of 1996
DHS – Department of Homeland Security
DIEMS – Date of Initial Entry into Military Service
DMO – Departmental Management and Operations
DNDO – Domestic Nuclear Detection Office
DOD – U.S. Department of Defense
DOI IBC – Department of the Interior's Interior Business Center
DOL – U.S. Department of Labor
E3A – EINSTEIN 3 Accelerated
EEI – Employee Engagement Index
EDS – Explosive Detection System
EMI – Emergency Management Institute
EO – Executive Order
ERM – Enterprise Risk Management
ERO – Enforcement and Removal Operations
FAA – DHS Financial Accountability Act
FBwT – Fund Balance with Treasury
FCRA – Federal Credit Reform Act of 1990
FDNS – Fraud Detection and National Security Directorate
FECA – Federal Employees Compensation Act of 1916
FEMA – Federal Emergency Management Agency
FERS – Federal Employees Retirement System
FEVB – Federal Employee and Veterans' Benefits
FEVS – Federal Employee Viewpoint Survey
FFMIA – Federal Financial Management Improvement Act of 1996
FIID – Fraud and Internal Investigations Division
FISMA – Federal Information Security Management Act
FLETC – Federal Law Enforcement Training Centers
FMFIA – Federal Managers' Financial Integrity Act
FSM – Financial Systems Modernization
FY – Fiscal Year
GAAP – Generally Accepted Accounting Principles
GAO – U.S. Government Accountability Office
GSA – General Services Administration
GSI – Global Satisfaction Index
HSGP – Homeland Security Grant Program
HRM – Human Resource Management
HSI – Homeland Security Investigations
HS-STEM – Homeland Security Science, Technology, Engineering, and Mathematics
I&A – Office of Intelligence and Analysis
ICE – U.S. Immigration and Customs Enforcement
IEFA – Immigration Examination Fee Account
IMATs – Incident Management Assistance Team
INA – Immigration Nationality Act

IP – Improper Payment  
IPERA – Improper Payments Elimination and Recovery Act of 2010  
IPERIA – Improper Payments Elimination and Recovery Improvement Act of 2012  
IPIA – Improper Payments Information Act of 2002  
IT – Information Technology  
JRC – Joint Requirements Council  
JTF – Joint Task Force  
MERHCF – Medicare–Eligible Retiree Health Care Fund  
MGMT – Management Directorate  
MHS – Military Health System  
MRS – Military Retirement System  
MTS – Metric Tracking System  
NCEPP – National Cyber Exercise and Planning Program  
NFIP – National Flood Insurance Program  
NPPD – National Protection and Programs Directorate  
NPSC – National Processing Service Centers  
NSSE – National Special Security Events  
OHA – Office of Health Affairs  
OIG – Office of Inspector General  
OMB – Office of Management and Budget  
OM&S – Operating Materials and Supplies  
OPA – Oil Pollution Act of 1990  
OPEB – Other Post Retirement Benefits  
OPM – Office of Personnel Management  
OPMAT – Operation Matador  
OPS – Office of Operations Coordination  
ORB – Other Retirement Benefits  
OSLTF – Oil Spill Liability Trust Fund  
PP&E – Property, Plant, and Equipment  
Pub. L. – Public Law  
PY – Prior Year  
RM&A – Risk Management and Assurance  
RFID – Radio Frequency Identification  
RNROC – Radiological/Nuclear Requirements Oversight Council  
RtF – Reduce the Footprint  
SAT – Senior Assessment Team  
SBR – Statement of Budgetary Resources  
SF – Square Feet  
SFFAS – Statement of Federal Financial Accounting Standards  
SFRBTF – Sport Fish Restoration Boating Trust Fund  
SMC – Senior Management Council  
SOS – Schedule of Spending  
SPR – State Preparedness Report  
S&T – Science and Technology Directorate  
TAFS – Treasury Account Fund Symbol  
TCM – Trade Compliance Measurement  
TCO – Transnational Criminal Organizations  
THIRA – Threat and Hazard Identification and Risk Assessment  
TSA – Transportation Security Administration  
TSGP – Transit Security Grants Program  
U.S. – United States  
USC – United States Code  
USCG – U.S. Coast Guard  
USCIS – U. S. Citizenship and Immigration Services  
USSS – U.S. Secret Service  
VA – U.S. Department of Veterans Affairs  
VP – Vendor Pay  
WYO – Write Your Own

# Acknowledgements

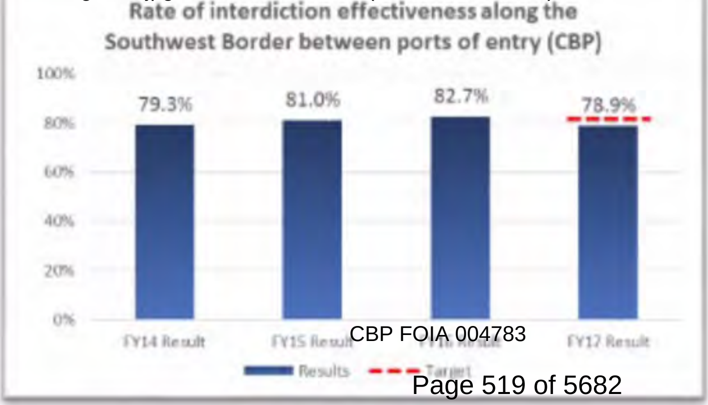
This Agency Financial Report (AFR) was produced with the tireless energies and talents of Department of Homeland Security Headquarters and Component employees and contract partners.

- Within the Office of the Chief Financial Officer, the division of Financial Management is responsible for financial management policy, preparing annual financial statements and related notes and schedules, and coordinating the external audit of the Department's financial statements.
- The division of Risk Management and Assurance provides direction in the areas of internal control to support the Secretary's assurance statement, risk management, and improper payments.
- The division of Program Analysis and Evaluation conducts analysis for the Department on resource allocation issues and the measurement, reporting, and improvement of DHS performance, and coordinates the Performance Overview section of the AFR.
- The division of GAO-OIG Audit Liaison facilitates Department relationships with audit organizations and coordinates with OIG on the Management Challenges report.

We offer our sincerest thanks to all Component financial management offices for their hard work and contributions.

Homeland Security

We are DHS



Rate of interdiction effectiveness along the Southwest Border between ports of entry (CBP)

From: [redacted] (b)(6);(b)(7)(C)

To: MCALEENAN, KEVIN K [redacted] (b)(6);(b)(7)(C)

VITIELLO, RONALD D (USBP) [redacted] (b)(6);(b)(7)(C)

FLANAGAN, PATRICK S [redacted] (b)(6);(b)(7)(C)

Cc: OC BRIEFING STAFF [redacted] (b) (7)(E) >; [redacted] (b)(6);(b)(7)(C)

Bcc:
Subject: AS1BB- 11.08.17
Date: Tue Nov 07 2017 17:10:44 EST
Attachments: AS1BB- 11.08.17.pdf

Attached is the Acting Secretary's Briefing Book for Wednesday, November 8, 2017.

[redacted] (b)(6);(b)(7)(C)

Program Manager, CBPTASKING & OC Briefing Staff

Office of the Executive Secretariat

U.S. Customs and Border Protection

[redacted] (b)(6);(b)(7)(C)

(b) (5)

[redacted]

(b) (5)

(b) (5)

(b) (5)

(b) (5)

[redacted]

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

[redacted]

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

[redacted]

(b) (5)

[redacted]

FOR OFFICIAL USE ONLY

(b) (5)

[redacted]

FOR OFFICIAL USE ONLY

(b) (5)

[redacted]

FOR OFFICIAL USE ONLY

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

[redacted]

(b) (5)

(b) (5)

(b) (5)

From: (b)(6);(b)(7)(C) [redacted]

To: MCALEENAN, KEVIN K (b)(6);(b)(7)(C) [redacted]
VITIELLO, RONALD D (USBP (b)(6);(b)(7)(C) [redacted]
FLANAGAN, PATRICK S (b)(6);(b)(7)(C) [redacted]

Cc: OC BRIEFING STAFF (b) (7)(E) [redacted] >;
(b)(6);(b)(7)(C) [redacted] >

Bcc:
Subject: AS2BB - 11.08.17
Date: Tue Nov 07 2017 16:25:04 EST
Attachments: AS2BB - 11.08.17.pdf

Attached, please find the AS2's Briefing Book for 11.08.17.

(b)(6);(b)(7)(C)

Program Manager, CBPTASKING & OC Briefing Staff

Office of the Executive Secretariat

U.S. Customs and Border Protection

(b)(6);(b)(7)(C)

(b) (5)

[redacted]

(b) (5)

[redacted]

(b) (5)

[redacted]

(b) (5)

(b) (5)

[redacted]

(b) (5)

[redacted]

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

~~FOR OFFICIAL USE ONLY~~

(b) (5)

FOR OFFICIAL USE ONLY

(b) (5)

(b) (5)

(b) (5)

[redacted]

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

[redacted]

(b) (5)

~~FOR OFFICIAL USE ONLY~~

(b) (5)

[redacted]

~~FOR OFFICIAL USE ONLY~~

(b) (5)

[redacted]

From: (b)(6);(b)(7)(C)

To: MCALEENAN, KEVIN K (b)(6);(b)(7)(C)
VITIELLO, RONALD D (USBP) (b)(6);(b)(7)(C)
FLANAGAN, PATRICK S (b)(6);(b)(7)(C)

Cc: OC BRIEFING STAFF (b) (7)(E)
>;
(b)(6);(b)(7)(C)
>

Bcc:
Subject: AS1BB- 11.07.17
Date: Mon Nov 06 2017 17:31:18 EST
Attachments: AS1BB- 11.07.17.pdf

Attached is the Acting Secretary's Briefing Book for Tuesday, November 7, 2017.

(b)(6);(b)(7)(C)

Program Manager, CBPTASKING & OC Briefing Staff

Office of the Executive Secretariat

U.S. Customs and Border Protection

(b)(6);(b)(7)(C)

(b) (5)

[redacted]

(b) (5)

~~FOR OFFICIAL USE ONLY~~

(b) (5)

[redacted]

(b) (5)

[redacted]

(b) (5)

[redacted]

(b) (5)

~~FOR OFFICIAL USE ONLY~~

(b) (5)

~~FOR OFFICIAL USE ONLY~~

(b) (5)

[redacted]

(b) (5)

(b) (5)

[redacted]

(b) (5)

[redacted]

(b) (5)

(b) (5)

| | | |
|---|---|---|
| ***O/R*** | Inter-Agency Coordination During a National Special Security Event | Walnut |

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

[redacted]

(b) (5)

(b) (5)

[redacted]

(b) (5)

[redacted]

(b) (5)

[redacted]

(b) (5)

|  |  |
|---|---|
| From: | [redacted] (b)(6);(b)(7)(C) |
| To: | FLANAGAN, PATRICK S [redacted] (b)(6);(b)(7)(C) |
| Cc: | FRIEL, MICHAEL J [redacted] (b)(6);(b)(7)(C)<br>>; ES COMMUNICATIONS & OUTREACH [redacted] (b) (7)(E)<br>[redacted] (b)(6);(b)(7)(C) |

(b)(6);(b)(7)(C)

Bcc:
Subject: RON NIXON NY TIMES ON DHS' GLOBAL REACH
Date: Mon Nov 06 2017 09:54:38 EST
Attachments: image001.jpg
image002.jpg
image003.jpg
image004.jpg
image005.jpg
image006.jpg
Thesis.pdf

Good morning,

CBP OPA recommends approval to support CBP's portion of NY Times' Ron Nixon's story about DHS' global reach and how, to keep our nation safe, DHS begins well-beyond U.S. borders. For CBP's part, our efforts in JIATF - South (P-3's) and our engagement in Kenya are the areas in which Mr. Nixon has particular interest.

As this is a DHS-wide story, Ass't. Sec'y Hoffman (DHS OPA) approved the engagement for all components involved (CBP, ICE, USCG, etc.). INA and AMO are both already aware and working with OPA on this project.

On the CBP engagement, access to our folks in INA and Nairobi to discuss CBP's efforts/engagements there, such as our canine training on interdicting wildlife products, and the PIO/Communicators training. Ron was part of a media panel at the training for Kenya PIOs in June here in Woodbridge, VA.

Ron has also requested a P-3 embark and OPA is coordinating with AMO for a flight to Costa Rica on Dec 1-3 and ASR. Ron will be travelling to Kenya following a personal trip to South Africa in mid-November and plans to be in Kenya Nov 20-24th.

We (OPA) are coordinating a pre-brief with INA for Ron prior to his travel to Kenya as well as for his engagement there as OPA will escort him in Kenya.

Ron has already spoken to AS1 (off the record) and interviewed several former CBP and ICE officials to include former ICE Director Hurd and former CBP Commissioners Kerlikowske and Aguilar.

Mr. Nixon revealed that he got his inspiration from a master's thesis written in June of this year by PAIC Christopher Seiler at National Defense University entitled: BIGFOOT OR BIG MISTAKE: IS CBP'S EXPANDING FOOTPRINT HELPING OR HURTHING HOMELAND SECURITY.

The abstract of that thesis:

"Bad actors and transnational criminal organizations have the ability to move illegal goods, drugs, dangerous materials, and people of interest to the "zero yard line" of the United States. Without a buffer to protect the homeland, limited people, time, and resources exist to

identify harmful items and individuals before they enter the U. S. and cause damage. The U. S. has relied on a geographical buffer and a positive relationship with Mexico and Canada in order to maintain our current security. Customs and Border Protection (CBP) has expanded their

division of International Affairs to build host country capacity, pre-clearance measures, and increased screening in foreign countries before arriving on the zero line. When it comes to securing the nation from those who would do it harm, CBP's global footprint is an efficient and

effective strategy not only to keep malevolent actors off the "zero yard line," but out of the "red zone" altogether. However, as with all deployments, these actions incur a fiscal and, unfortunately, human cost as some agents are killed in IED and Blue on Green attacks, leaving

some to ask: are such forward deployments worth their cost? Are they the most effective way to secure the U.S.?"

Very respectfully,

(b)(6);(b)(7)(C)

Director, Media Division

Office of Public Affairs

U.S. Customs and Border Protection

Office: (b)(6);(b)(7)(C)

iPhone: (b)(6);(b)(7)(C)

# REPORT DOCUMENTATION PAGE

*Form Approved*
*OMB No. 0704-0188*

| | | |
|---|---|---|
| 1. REPORT DATE *(DD-MM-YYYY)*<br>31-03-2017 | 2. REPORT TYPE<br>Master's Thesis | 3. DATES COVERED *(From - To)*<br>from 08-01-2016 to 06-15-2017 |

4. TITLE AND SUBTITLE

**BIGFOOT OR BIG MISTAKE: IS CBP'S EXPANDING FOOTPRINTHELPING OR HURTING HOMELAND SECURITY?**

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

**Christopher M. Seiler**
**Patrol Agent in Charge**
**United States Border Patrol**

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) AND ADDRESS(ES)

**National Defense University**
**Joint Forces Staff College**
**Joint Advanced Warfighting School**
**7800 Hampton Blvd**
**Norfolk, VA 23511-1702**

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

**U. S. Customs and Border Protection**
**1300 Pennsylvania Ave., NW**
**Washington, D.C. 20029**

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

**Approved for public release, distribution is unlimited.**

13. SUPPLEMENTARY NOTES

**Not for commercial use without the express written permission of the author.**

14. ABSTRACT

Bad actors and transnational criminal organizations have the ability to move illegal goods, drugs, dangerous materials, and people of interest to the "zero yard line" of the United States. Without a buffer to protect the homeland, limited people, time, and resources exist to identify harmful items and individuals before they enter the U. S. and cause damage. The U. S. has relied on a geographical buffer and a positive relationship with Mexico and Canada in order to maintain our current security. Customs and Border Protection (CBP) has expanded their division of International Affairs to build host country capacity, pre-clearance measures, and increased screening in foreign countries before arriving on the zero line. When it comes to securing the nation from those who would do it harm, CBP's global footprint is an efficient and effective strategy not only to keep malevolent actors off the "zero yard line," but out of the "red zone" altogether. However, as with all deployments, these actions incur a fiscal and, unfortunately, human cost as some agents are killed in IED and Blue on Green attacks, leaving some to ask: are such forward deployments worth their cost? Are they the most effective way to secure the U.S.?

15. SUBJECT TERMS

**Border, Customs and Border Protection, Terrorism, U.S. Border Patrol**

| | | | | | |
|---|---|---|---|---|---|
| 16. SECURITY CLASSIFICATION OF:<br>**Unclassified** | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON<br>**Stephen C. Rogers, Colonel, USA**<br>**Director, Joint Advanced Warfighting School** |
| a. REPORT<br>**Unclassified** | b. ABSTRACT<br>**Unclassified** | c. THIS PAGE<br>**Unclassified** | **Unclassified/ Unlimited** | **48** | 19b. TELEPHONE NUMBER |

**Standard Form 298 (Rev. 8-98)**
**Prescribed by ANSI Std. Z39.18**

NATIONAL DEFENSE UNIVERSITY

JOINT FORCES STAFF COLLEGE

JOINT ADVANCED WARFIGHTING SCHOOL

# BIGFOOT OR BIG MISTAKE: IS CBP'S EXPANDING FOOTPRINT HELPING OR HURTING HOMELAND SECURITY?

by

**Christopher M. Seiler**

**Patrol Agent in Charge**

**United States Border Patrol**

This Page Intentionally Left Blank

# BIGFOOT OR BIG MISTAKE: IS CBP'S EXPANDING FOOTPRINT HELPING OR HURTING HOMELAND SECURITY?

**BY**

**Christopher M. Seiler**

**Patrol Agent in Charge**

**United States Border Patrol**

**A paper submitted to the Faculty of the Joint Advanced Warfighting School in partial satisfaction of the requirements of a Master of Science Degree in Joint Campaign Planning and Strategy. The contents of this paper reflect my own personal views and are not necessarily endorsed by the Joint Forces Staff College or the Department of Defense.**

**This paper is entirely my own work except as documented in footnotes.**

Signature: ____________________

**31 March 2017**

**Thesis Advisor:** Signature: ____________________

**Dr. Bryon Greenwald, Ph.D.**
**Professor, JAWS**

**Approved by:** Signature: ____________________

**James D. Golden, Col. USAF**
**Committee Member, JAWS**

Signature: ____________________

**Stephen C. Rogers, COL, USA**
**Director, JAWS**

This Page Intentionally Left Blank

# ABSTRACT

Bad actors and transnational criminal organizations have the ability to move illegal goods, drugs, dangerous materials, and people of interest to the “zero yard line” of the United States. Without a buffer to protect the homeland, limited people, time, and resources exist to identify harmful items and individuals before they enter the U. S. and cause damage. The U. S. has relied on a geographical buffer and a positive relationship with Mexico and Canada in order to maintain our current security. Customs and Border Protection (CBP) has expanded their division of International Affairs to build host country capacity, pre-clearance measures, and increased screening in foreign countries before arriving on the zero line. When it comes to securing the nation from those who would do it harm, CBP’s global footprint is an efficient and effective strategy not only to keep malevolent actors off the “zero yard line,” but out of the “red zone” altogether. However, as with all deployments, these actions incur a fiscal and, unfortunately, human cost as some agents are killed in IED and Blue on Green attacks, leaving some to ask: are such forward deployments worth their cost? Are they the most effective way to secure the U.S.?

## DEDICATION

I would like to thank my Thesis advisors, Dr. Bryon Greenwald and Col. Doug Golden, USAF, for their continued assistance and guidance in this academic endeavor. Second, I want to thank my Seminar Two instructors, Col. Kevin Therrian, Professor Dave Rodermill, and Professor Mary Bell for their knowledge, humor, and dedication to making our seminar a success. Lastly, my Seminar Two classmates who have made the academic rigors of JAWS, behind the scenes learning, and off time a lifelong, enjoyable experience.

# TABLE OF CONTENTS

This Page Intentionally Left Blank

## INTRODUCTION

Contrary to common perception, the U.S. Customs and Border Protection (CBP) does not just operate border control points and port of entry clearance areas. CBP personnel are deployed globally expanding the boundaries of security and training others to help keep America safe. For example, in 2005, in Asuncion, the capital city of Paraguay, a U.S. Border Patrol Agent spoke to Paraguayan Customs, Navy personnel, and multiple media outlets about Paraguay's importance in the Western Hemisphere's security. Known as the Heart of South America, Paraguay is part of the infamous Tri-Border Region, an area of South America notorious as a cross-roads for terrorists and transnational criminal organizations (TCOs). This stands as a clear example of CBP's strategy to accomplish its mission globally.

Similarly, in support of USCENTCOM, CBP agents deployed with servicemen to Iraq and Afghanistan to assist those nations in providing for their border security while simultaneously enhancing security at home by thwarting the movement of drugs, terrorists, dangerous materials, and human trafficking through those countries. As with all deployments, these actions incurred a fiscal and, unfortunately, human cost as some agents were killed in IED and Blue on Green attacks, leaving some to ask: are such forward deployments worth their cost? Are they the most effective way to secure the U.S.?

Due to the elevated security risk to the United States, U.S. Customs and Border Protection (CBP) is expanding its global footprint overseas to increase the level of security of the homeland, reduce transnational crime, and facilitate trade and travel. This will be accomplished through foreign nation capacity building, pre-clearance measures, and increased screening. This analysis of historical events, current methods, and future threats validates CBP's international mission and recommends additional action to increase U.S. security. When it comes to securing the nation from those who would do it harm, CBP's global footprint is an efficient and effective strategy not only to keep malevolent actors off the "zero yard line," but out of the "red zone" altogether.

# CHAPTER 1

## Origins of DHS, CBP, and Expanding Footprint

> *Borders are heaven, they are nirvana for traffickers and for the illicit networks in which they function.*[1]
>
> *Michael Miklaucic*
> *Director, Center for Complex Operations*

The morning was just like every other morning; people took their kids to work, others were on their way for their morning coffee, and the United States lived in an isolationist bubble. A new, soon to be appointed, government employee reported for his second day in Washington, DC. Robert C. Bonner had reported for duty, but had yet to be confirmed by the U.S. Senate as the Commissioner for the U.S. Customs. At that time, U.S. Customs resided under the Treasury Department. Commissioner Bonner and the lives of everyone else in the country were about to change indefinitely. At 9:35 am, hijackers flew two commercial airplanes into the World Trade Center in New York City, one into the Pentagon in Northern Virginia, and a fourth planned to fly into the U.S. Capitol. This act of foreign grown terrorism on U.S. soil had horrific effects on the nation with 2,933 innocent lives taken. A number of changes were to come that would reverberate through the rest of U.S. history, including the invasion of Afghanistan and Iraq, the creation of the Department of Homeland Security (DHS), a change in the way the U.S. combatted terrorism, and the loss of a nation's innocence.

Immediately after the attacks, Commissioner Bonner knew that a change in the mission of U.S. Customs Service was essential to the survival of the U.S. Bonner made the dramatic change in the priority mission of Customs from interdiction of drugs and regulation of trade to

[1] Michael Miklaucic and Moises Naim, "The Criminal State," in *Convergence: Illicit Networks and National Security in the Age of Globalization (*Washington, D.C.: National Defense University Press, 2013), 149.

preventing terrorists and terrorist weapons from getting into the United States. This led to a number of changes that will be discussed later in the paper, but the first step was to refocus the agency and personnel as a whole. Commissioner Bonner began his third day with an all hands meeting of U.S. Customs employees worldwide. He emphasized the importance of the attacks and how the priority mission had changed to preventing terrorist and terrorist weapons from entering the United States.[2] The U.S. had been lulled into a false sense of security by the illusion that the vast oceans that surround the country and its relationship with peaceful neighbors would protect the nation. This idea of containment and mutual deterrence against this type of enemy was obviously not effective; a change had to be made. The United States, under President George Bush, took a three-pronged approach both to fighting the terrorist threat against the U.S. and global terrorism in general. First, the U.S. would go on the offensive and go after the terrorists, their leaders, and the countries that harbor them. Second, the U.S. would have a strong, coordinated defense of the homeland, which led to the formation of the new Department of Homeland Security. Lastly, the U.S. would begin an aggressive information operation campaign to undermine the jihadi message.

Since its founding in 1789, the U.S. Customs Service has guarded the U.S. ports of entry and collected tariffs on goods coming into the United States. In 1924, the U.S. Border Patrol was created primarily to stop illegal entries along the U.S.-Mexico and Canadian International Borders.[3] Each agency held a similar mission of protecting the nation's borders, but were under different parent agencies. After the tragedy of September 11, 2001, Congress created the Department of Homeland Security, and both agencies merged to form U. S. Customs and Border

[2] Robert C. Bonner, "Securing the transnational movement of trade and people in the era of global terrorism." *Strategic Insights,* June 2006, 2-4.
[3] U.S. Customs and Border Protection. "About CBP."

Protection (CBP). It is now the mission of CBP “to safeguard America's borders thereby protecting the public from dangerous people and materials while enhancing the Nation's global economic competitiveness by enabling legitimate trade and travel.”[4] It is now understood by the U.S. government and its citizens that the U.S. must “take the fight” to the people who are attempting to do the U.S. harm. Although on a smaller scale, CBP has a direct parallel to the Department of Defense and the “War on Terror” in order to prevent attacks on the homeland. CBP is expanding into foreign countries to be more effective and keep the bad actors away from U.S. soil.

In order to fulfill the requirements of President Bush’s three-pronged strategy, an aggressive reorganization of the defense of the homeland took place. The formation of the Department of Homeland Security was the largest reorganization of the federal government since 1947. The Homeland Security Act of 2002 (P.L. 107-296) created a framework for the transfer of all or part of 22 different federal agencies into the newly formed Department of Homeland Security (DHS). This included the U.S. Customs Service, U.S. Border Patrol, and U.S. Coast Guard. Title IV of the Act created the Directorate of Homeland Security headed by the Under Secretary for Border and Transportation Security.[5] The Directorate was tasked with three responsibilities:

- Prevent the entry of terrorists and the instruments of terrorism into the U. S.;
- Ensure the speedy, orderly, and efficient flow of lawful traffic and commerce and;
- Establish the U.S. Customs Service and the office of Customs within DHS.

[4] U.S. Customs and Border Protection, *Vision and Strategy 2020*, (Washington DC: Government Printing Office, 2014), 7.

[5] Sec. 401 of P.L. 107-296; 6 U.S.C. 70114

The Homeland Security Act directed the President to reorganize the agencies under DHS no later than 60 days from the enactment. This moved personnel, assets, and obligations from the 22 affected agencies into DHS (See Figure 1). Part of this reorganization was the formation of a “One Border Agency” idea, which became U. S. Customs and Border Protection (CBP). In addition, the U.S. Customs Service was renamed the Bureau of Customs and Border Protection (CBP) and was to include the Office of Field Operations (OFO), U.S. Border Patrol (USBP), and later the Office of Air and Marine (OAM).[6]

The Homeland Security Act accomplished a number of goals. First, it abolished a broken Immigration and Naturalization Service (INS), which had issued visas to several of the 9/11 terrorist hijackers six months after the attacks on America. The duties of the INS were divided and streamlined among the new DHS agencies to prevent further mistakes. Second, it combined the personnel from the United States Border Patrol, previously under the Department of Justice, with the U.S. Customs Service and the border inspectors of the U.S. Department of Agriculture under the new CBP banner.[7] This allowed for one single agency to manage, control, and secure the nation’s borders to include all the official ports of entry and the area between these ports for

[6] On the establishment of the Department of Homeland Security, see archived CRS Report RL 31549*, Department of Homeland Security: Consolidation of Border and Transportation Security Agencies*, by Jennifer E. Lake; and archived CRS Report RL31493*, Homeland Security: Department Organization And Management—Legislative Phase,* by Harold C. Relyea.

[7] U.S. Congress, House, Committee on Homeland Security, Reorganization Plan Modification for the Department of Homeland Security, Communication from the President of the United States, House Document 108-32, 108th Cong., 1st sess., February 3, 2003.

the purposes of preventing terrorist and terrorist weapons (bio and agro terrorism included) from entering the country, while promoting legitimate trade and travel.

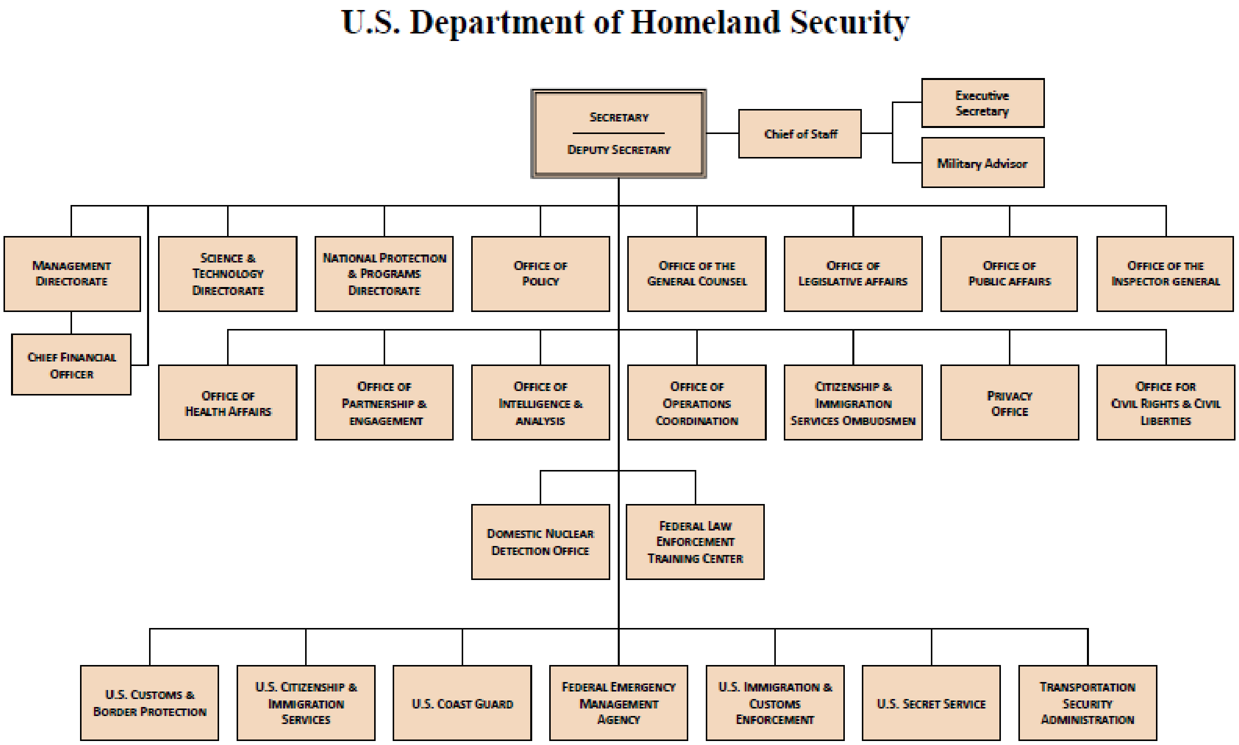

U.S. Department of Homeland Security
Secretary
Deputy Secretary
Chief of Staff
Executive Secretary
Military Advisor
Management Directorate
Chief Financial Officer
Science & Technology Directorate
National Protection & Programs Directorate
Office of Policy
Office of the General Counsel
Office of Legislative Affairs
Office of Public Affairs
Office of the Inspector General
Office of Health Affairs
Office of Partnership & Engagement
Office of Intelligence & Analysis
Office of Operations Coordination
Citizenship & Immigration Services Ombudsmen
Privacy Office
Office for Civil Rights & Civil Liberties
Domestic Nuclear Detection Office
Federal Law Enforcement Training Center
U.S. Customs & Border Protection
U.S. Citizenship & Immigration Services
U.S. Coast Guard
Federal Emergency Management Agency
U.S. Immigration & Customs Enforcement
U.S. Secret Service
Transportation Security Administration

FIGURE 1. U.S. Department of Homeland Security[8]

On an average day, CBP welcomes to the United States on average one million travelers and visitors via land, air, and sea ports of entry (POE's).[9] As the threats against the U.S. have increased over the last two decades, CBP has had to increase the buffer around the nation and not view the nation's borders as the only line of defense. A new approach being taken in concert with the nation's international partners is to create a multi-layered, intelligence driven strategy. This new strategy encompasses every aspect of CBP's mission and capabilities to ensure safe

[8] U.S. Department of Homeland Security. "About DHS." https://www.dhs.gov/sites/default/files/publications/Department%20Org%20Chart_1.pdf

[9] U.S. Congress. Written Testimony of CBP Office of Field Operations Deputy Assistant John Wagner for House Committee on Homeland Security, Subcommittee on Border and Maritime Security Hearing Titled' The Outer Ring of Border Security: DHS's International Security Programs. *States News Service*, 2015. *Biography in Context*.

travel for airline passengers from the time a passenger books or purchases a ticket, to inspecting travel documents, at the airport, while in route, and upon arrival in the U.S. POE's or equivalent.

After the events of 9/11, the United States can no longer remain at home; it must go on the offensive and take the fight to the terrorists who attacked the country. The questions is, "What is the best way to do this?" A number of theories developed on how best to keep the homeland secure, one technique was through deterrence operations. Deterrence operations convince the adversaries not to take actions that threaten U.S. vital interests by means of decisive influence over their decision making. This influence is achieved by credibly threatening to deny benefits and/or imposing cost, while encouraging restraint by convincing the actor that restraint will result in acceptable outcomes.[10]

Customs and Border Protection's capabilities in forward stationed and forward deployed areas enhance deterrence by improving the ability to act in the host nation country, as opposed to being on the zero-line. This forward presence strengthens the role of partners and expands joint and multi-national capabilities. CBP presence conveys a credible message that the U.S. will remain committed to preventing conflict and demonstrates commitment to the defense of the U.S. and strategic partners. This demonstration of U.S. political will and resolve shows that there is opposition to adversary aggression and coercion in the regions that are important to U.S. formal alliances and security relationships.[11] These critical relationships are determined by U.S. National Interests and the strategic areas in which CBP can provide the most impact against combatting transnational criminal organizations.

[10] Deterrence Operations*, Joint Operating Concept, Version 2.0* December 2006, 26-28.
[11] Ibid., 33.

# Chapter 2

## Transnational Criminal Organizations: An Evolving Threat

*Just as legitimate governments and businesses have embraced advances of globalization, so too have illicit traffickers harnessed the benefits of globalization to press forward their illicit activities.*

*Admiral James Stavridis*

Over the past decade, U.S. officials have learned that one of the biggest threats to national and international security is the development and expansion of Transnational Organized Crime (TCO). As defined by the July 2011 Strategy to Combat Transnational Organized Crime, the term, transnational organized crime, more accurately describes the emerging threat America faces today. As emphasized by the National Security Strategy, "…These threats cross borders and undermine the stability of nations, subverting government institutions through corruption and harming citizens worldwide."[12] The goal of the July 2011 Strategy to Combat Transnational Organized Crime is to reduce transnational organized crime from a national security threat to a manageable public safety problem in the U.S. and in strategic regions around the world. This will be accomplished by achieving five key policy objectives:

1) Protect American and our partners from the harm, violence, and exploitation of transnational criminal networks.

2) Help partner countries strengthen governance and transparency, break the corruptive power of transnational criminal networks, and sever state-crime alliances.

3) Break the economic power of transnational criminal networks and protect strategic markets and the U.S. financial system from TOC penetration and abuse.

[1] U.S. President, *Strategy to Combat Transnational Organized Crime: Addressing Converging Threats to National Security* (Washington DC: Government Printing Office, July 2011), 2-5.

4) Defeat transnational criminal networks that pose the greatest threat to national security by targeting their infrastructures, depriving networks of the means which enable them, and preventing the criminal facilitations of terrorist activities.

5) Build international consensus, multilateral cooperation, and public-private partnerships to defeat transnational organized crime. [2]

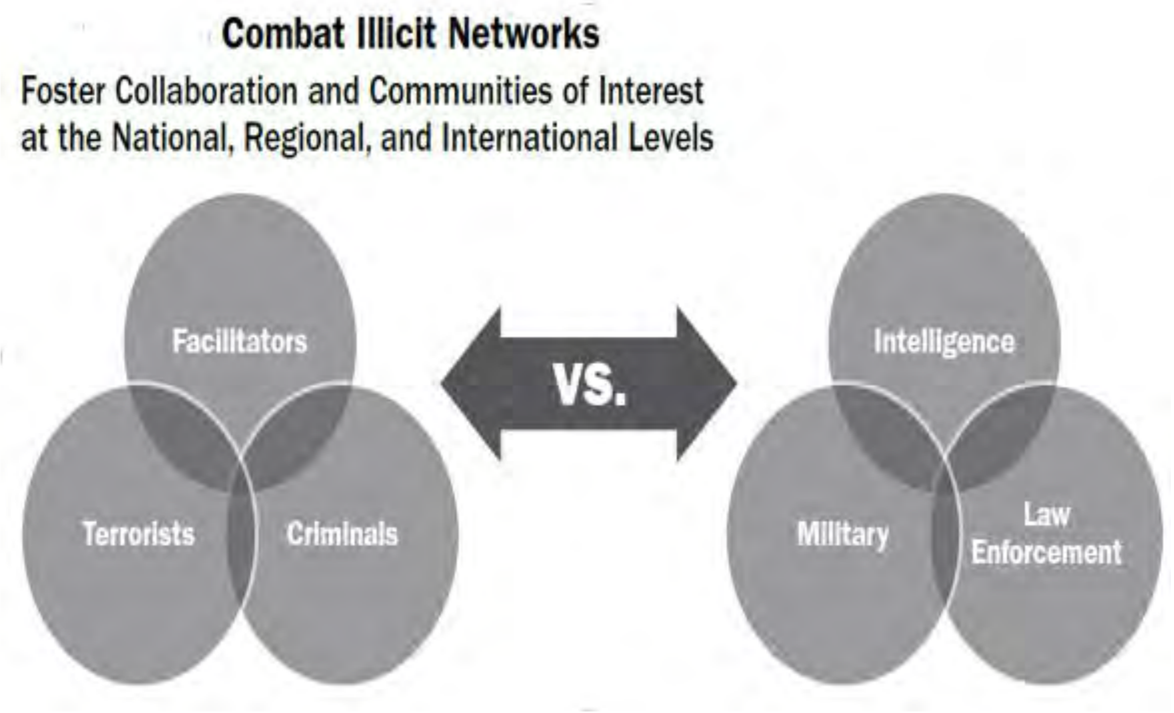

Combat Illicit Networks
Foster Collaboration and Communities of Interest at the National, Regional, and International Levels
Facilitators
Terrorists
Criminals
VS.
Intelligence
Military
Law Enforcement

FIGURE 3. [3]

Bad actors and transnational criminal organizations have the ability to move illegal goods, drugs, dangerous materials, and people of interest to the "zero yard line" of the United States. Without a buffer to protect the homeland there are limited people, time, and resources to identify harmful items and individuals before they enter the U. S. and cause damage. The U. S. has relied on a geographical buffer and a positive relationship with Mexico and Canada in order to

[2] Ibid.

[3] Celina B. Realuyo, "Collaborating to Combat Illicit Networks Through Interagency and International Efforts," in *Convergence: Illicit Networks and National Security in the Age of Globalization (*Washington, D.C.: National Defense University Press, 2013), 263.

maintain its current security. The attacks on 9/11 proved that the buffer that had protected the U.S. has disappeared. Accordingly, CBP has expanded its division of International Affairs to build host country capacity, establish pre-clearance measures, and increase screening in foreign countries before arriving on the zero line.

CBP's expansion into a number of foreign countries is a bold and potentially dangerous move that could have negative repercussions. There are three major concerns with this expansion:

> 1) Cost. Is it fiscally responsible to have personnel detailed long term or permanently moved to these countries, along with the high cost of training for the employees and host nation personnel? Is it worth human lives and human capital to be deployed overseas as opposed to in the homeland?
>
> 2) Culturally. Does it have a negative impact on the host nation country and build negative stereotypes of Americans?
>
> 3) Operational Effectiveness. Does it detract from the mission at home and what is the effectiveness in the U. S. and overseas?

An extensive review of current literature relating to terrorism, transnational crime, and threats to U.S. trade and travel suggests that the expanding footprint is effective in protecting the homeland. These actions have had positive and negative effects on XX, but as interviews with CBP personnel and an in depth analysis of data shows the net effect is to increase America's security.[4]

Fifteen years after 9/11, it is still evident that the fight is not over, but America is making progress as noted in the alignment of missions between the National Security Strategy, the Department of Defense, and CBP. In his 2015 National Security Strategy President Obama

[4] U.S. Congress. Written Testimony of CBP Office of Field Operations Deputy Assistant John Wagner for House Committee on Homeland Security, Subcommittee on Border and Maritime Security Hearing Titled "The Outer Ring of Border Security: DHS's International Security Programs." *States News Service*, 2015. *Biography in Context*.

wrote that, "our obligations do not end at our borders," that the U. S. must "uphold our commitment to allies and partners," and that "fulfilling our responsibilities depends on a strong defense and secure homeland."[5] President Obama's message was previously laid out in the Quadrennial Defense Review 2014 for the priorities of the Department of Defense illustrating its importance. The Department's strategy empathized three pillars:

- Protect the homeland, to deter and defeat attacks on the United States and to mitigate the effects of potential attacks and natural disasters.
- Build security globally, preserve regional stability, deter adversaries, support allies and partners, and cooperate with others to address common security challenges.
- Project power and win decisively to defeat aggression, disrupt and destroy terrorist networks, and provide humanitarian assistance and disaster relief.[6]

The three pillars of the Department of Defense (DOD) compliment the mission of Customs and Border Protection (CBP) and work in concert for a whole of government approach to protect U.S. national interests and security.

After the creation of DHS and the reorganization of CBP, the next step was to go on the offensive and extend the U.S. zone of security to interdict and deter threats on foreign soil as far away from the homeland as possible and to not allow the U.S. border to be the zero yard line. This was accomplished through expanding the global footprint and improving three critical areas: 1) Enforcement, 2) System and technology upgrades, and 3) Training. All of this needed to take place on foreign soil with the assistance and agreement of the host nation.[7]

[5] U.S. President, national Security Strategy (Washington DC: Government Printing Office, February 2015), 8.
[6] Quadrennial Defense Review, (Washington DC: Government Printing Office, May 2014), 4.
[7] Robert Bonner. "Securing the transnational movement of trade and people in the era of global terrorism." *Strategic Insights Series, June 2006,* 18-19.

# CHAPTER 3

## CBP's Expanded Footprint and How to Protect the Homeland

To extend the zone of security away from the homeland, CBP implemented a new risk based layered approach. This new strategy employed innovative pre-departure security efforts before people or products departed their foreign ports. One of the key supporting capabilities is the National Targeting Center (NTC), which receives advanced passenger information identifying potential risks at the earliest time possible. CBP then works in concert with the host nations including those in Europe, North Africa, and the Middle East to provide greater situational awareness for host countries. The information provided and generated by the NTC can be utilized by CBP's overseas enforcement programs, Pre-clearance Immigration Advisory, and Joint Security Programs and Regional Carrier Liaison Groups to combat threats before they occur (these programs will be addressed in more detail later). The NTC, utilizing a whole of government approach, works closely with their parent agency, DHS and components, the Department of State, Department of Defense, and the Intelligence community to leverage all the assets, jurisdictions, and authorities to identify and address these security threats.[1]

Although CBP's expansion has been successful, there have been some friction points that are continually being reworked. In December 2001, DHS Secretary Tom Ridge and Canadian Deputy Prime Minister John Manley signed the "Smart Border" Declaration and associated 30-point action plan to enhance the security of our shared border while facilitating the legitimate flow of people and goods. Some of the associated 30 point actions items included clearance away

[1] U.S. Congress. Written Testimony of CBP Office of Field Operations Deputy Assistant John Wagner for House Committee on Homeland Security, Subcommittee on Border and Maritime Security Hearing Titled "The Outer Ring of Border Security: DHS's International Security Programs." *States News Service*, 2015. *Biography in Context*.

from the border, immigration officers overseas, and international cooperation. Since the implementation of the Bush Administration strategy of smart borders there has been resistance by some countries, especially in Europe.[2] The international community argued that the U.S. imposed new rules on their airlines, people, and countries. The use of biometric identifiers are viewed as an intrusion on Europeans' personal data. Another debate that arose was the extra cost to the private sector because of the newly implemented extensive controls on container security. A number of other challenges that have been identified, including legal challenges concerning extraterritorial laws, internal politics within strategic partners, and implementing processes in the private sector. The Transatlantic shift and cooperation with Europe needs to be more thoroughly developed for both to mutually benefit from a global homeland security network.[3]

### Extending the Zone of Security/Targeting and Detecting Risk (Whole of Governments Approach)

CBP extended the zone of security for the homeland using a risk based, layered approach that pushes the U.S. border security efforts outward to detect, assess, and mitigate risks posed by travelers, materials, or other threats before they reach the borders of the U.S. The Pre-departure process integrates multiple levels of capabilities and programs that form an overlapping strategy along the travel cycle of passengers and cargo. This strategy ensures that threats are detected as early as possible, while assisting the host nation country by ensuring they are also kept safe.[4] Working through the pre-departure process and throughout the international cycle, CBP is

[2] Gerhard Peters and John T. Woolley, “Summary of Smart Border Action Plan Status.” *The American Presidency Project,* September 9, 2002. http://www.presidency.ucsb.edu/ws/?pid=79762Online by Gerhard Peters and John T. Woolley (accessed December 27, 2016).

[3] Patryk Pawlak, "Transatlantic homeland security cooperation: the promise of new modes of governance in global affairs." *Journal of Transatlantic Studies* 8, no. 2 (Summer 2010): 139-157.

[4] *Congressional Research Service, U.S. Customs and Border Protection: Trade Facilitation, Enforcement, and Security, by the Congressional Research Service,* March 2013 (Washington, DC: Government Printing Office, 2013), 28-40.

working with the host nation, foreign partners, and other U.S. government agencies. CBP works closely with the other components of the Department of Homeland Security (DHS), the Department of State (DOS), the Department of Defense (DOD), and the intelligence community to ensure that all assets and resources are leveraged and emerging threats are identified early. On a daily basis, CBP personnel from the National Targeting Center (NTC), work with our partners in Europe, North Africa, the Middle East, and those from the Five Eyes countries (U.S., United Kingdom, Australia, Canada, and New Zealand). Specifically, two major processes can be impacted through the extended zone of security: passenger measures and cargo measures. Both have different threats to the security of the homeland and will be broken down for a more close examination.

## Passenger Measures

Passenger identification and travel security has always been a security risk/concern for customs agencies all over the world. The risk of hijackings in the 1980s and the use of a plane as a weapon on 9/11 illustrated how the system needed to be greatly improved. A number of new measures were implemented to make passenger travel more secure.

### Visa and Travel Authorization Security

One of the first steps in legal, international travel is to obtain the proper documents to travel abroad. This means applying for a passport, visa, travel authorizations, and the proper boarding documents. Most foreign nationals must apply for a non-immigrant visa through a U.S. Embassy or Consulate. The burden of the visa application and adjudications process lies within the Department of State, however, CBP also conducts vetting of these visas. CBP does this through the National Targeting Center and continuously vets non-immigrant visas that have been issued, revoked, or denied. If a traveler's status changes, this rechecking ensures the traveler will not be allowed to board the conveyance. This is accomplished through heightened screening efforts with U.S. Immigration and Customs Enforcement (ICE) and the Department of State (DOS). An enhanced, automated screening system continually monitors the traveler's life cycle through their travel process. This has revolutionized and streamlined the way the U.S. government can monitor foreign nationals looking to enter the U.S. This process is a precursor system and works in tandem with DOS Security Advisory Opinion (SAO) and Advisory Opinion (AO) programs. The collaboration of the three agencies ensures the broadest of jurisdictions, authorities, expertise, and technologies to examine every passenger a number of times and through their travel. [5]

Pre-Clearance Operations

Pre-Clearance operations are CBP's highest level of overseas ability to detect, prevent, and apprehend individuals on foreign soil prior to departure for the United States. Inspection and clearance of commercial passengers overseas ensures the U.S.'s extended border strategy. This is accomplished through uniformed CBP officers with legal authority to question and inspect travelers and luggage in foreign airports. The officers complete the same immigration, customs, and agricultural inspections of passengers at foreign airports as are performed at domestic ports of entry. Passengers that are found inadmissible at the gate are not allowed to board the aircraft and travel to the U.S. This also provides cost savings to the USG because the cost of returning the individual is no longer needed. In Fiscal Year 2014, this saved approximately $50 million dollars and kept air travel safer.[6] Passengers that do pass inspection abroad are not required to

[5] "The Outer Ring of Border Security: DHS's International Security Programs." *States News Service*, 2015.
[6] Ibid.

pass any other inspection requirements upon arriving at a U.S. airport. This decreases time and increases efficiency for travelers, carriers, and airports.

Pre-clearance operations are currently in Canada, Ireland, The Bahamas, Aruba, and the United Arab Emirates. In 2014, CBP officers pre-cleared 17.4 million travelers, which accounted for 21% of all commercial aircraft inbound to the U.S. from the participating countries. Most importantly, with the respect to terrorist threats from the Middle East, the UAE receives flights from Yemen, Morocco, Nigeria, Kenya, Ethiopia, Sudan, Saudi Arabia, Pakistan, Iraq, Lebanon, Bangladesh, and India enroute to the U.S. All of these countries are high-risk pathways for terrorist travel and terrorists from these countries seek to utilize the UAE to bypass other security measures for entry into the U.S. and Europe. CBP officers in pre-clearance country airports are enabled with technology, access to data bases, and granted full inspection authority with regard to travelers and baggage. If discovered to be questionable by CBP personnel and in need of additional screening, individuals can be further investigated by DHS's Homeland Security Investigations (HSI) or the Federal Bureau of Investigation (FBI) in the host country or once arriving in the U.S.

Immigration Advisory Program (IAP) and Joint Security Program (JSP)

Two additional levels of the layered approach to passenger security before boarding the plane include the Immigration Advisory Program (IAP) and the Joint Security Program (JSP). These programs use advanced information from the NTC to identify possible terrorists and high-risk passengers. CBP Officers are posted at major gateway airports in Western Europe, Asia, and the Middle East, including Amsterdam, Frankfurt, London, Madrid, Paris, Tokyo, Mexico City, Panama City, and Doha. The CBP Officers work with the host nation countries to identify passengers linked to terrorism, narcotics, weapons, and currency smuggling. Once an individual is identified, officers issue a no-board recommendation to the commercial carriers, which prevents the improperly documented travelers from boarding flights destined for the U.S. One limit to the program is that the officers do not have the legal authority to require the air carrier not to allow the passenger on the flight. Therefore, cooperation between the host nation, the airline, and the CBP officers is a must for the program to succeed. The recommendations are generally accepted and followed by the airlines.

### CBP Carrier Liaison Program (CLP)

All of the weight of secure air travel does not fall on CBP alone. The commercial airlines and CBP realize that the safety of their passengers is important to everyone and developed the Carrier Liaison Program (CLP). Specially trained CBP officers train commercial air carrier participants to identify, detect, and disrupt improperly documented passengers. This process can identify passengers in-flight for further inspection upon landing and have their fraudulent documents removed from circulation. Since the start of the program, CBP has provided training to more than 34,800 airline industry personnel. This program, along with host nation participation, exponentially increases the number of people watching for illegal activity and improves the security of the passengers and homeland.

### The Pre-Departure

Pre-Departure Targeting starts well before the passenger arrives at an airport attempting to enter the U.S. When a traveler books a ticket to travel to the U.S. a Passenger Name Record (PNR) and Advance Passenger Information System (APIS) entry is generated in the airlines' reservations system. This information includes itineraries, co-travelers, changes to the reservation, and payment information. This information is then cross-referenced with criminal history, records of lost or stolen passports, public health records, visa refusals, prior immigration violations intelligence reports, law-enforcement data bases, and the Terrorist Screening Database (TSDB). Pre-Departure Targeting can prohibit someone from boarding the plane. If permitted to travel, further investigation continues while in-flight in order to provide more inspection upon entry to the U.S.[7]

In addition, if fraudulent, counterfeit, or altered travel documents are discovered, the documents are removed from circulation and sent to CBP's Fraudulent Document Analysis Unit (FDAU). The FDAU is a central depository and analysis center for seized documents. The FDAU can provide intelligence, alerts to field operations, and up to date pertinent training for field units on current tactics, techniques, and procedure for fraudulent documents. These functions along with removing the fraudulent document and the detaining the traveler provide another layer of enforcement along with prevention of future misuse.

Arrival Processing and Trusted Travelers

CBP's layered approach not only provides additional layers of enforcement, but also identifies low-risk travelers to facilitate speedy travel. CBP's Global Entry Program provides for expedited processing upon arrival in the U.S. for pre-approved, low-risk participants. This is accomplished through the use of secure Global Entry kiosks that have machine-readable passports technology, a fingerprint scanner, along with a complete customs declaration. Once approved, the traveler is issued a transaction receipt and directed to the baggage claim and the exit. In order to be a member of the Global Entry Program a rigorous background check and in-person interview is conducted before enrollment. Any violation of the program's terms and

[7] Ibid.

conditions results in termination of the traveler's privileges and appropriate enforcement measures.

## Cargo Measures

The second element and equally dangerous to national security is the risk of dangerous goods and material coming into the country. Weapons of mass destruction coming into the country without being detected, human smuggling, and legitimate trade with customs not being documented or paid all present significant risk and potential cost to the U.S. The following portion of the paper will illustrate how CBP's expanded footprint mitigates and identifies these concerns.

### Container Security Initiative (CSI)

The Container Security Initiative (CSI) is a collaboration between CBP, Immigrations and Customs Enforcement (ICE), and host nation law enforcement agencies in CSI countries. Advanced Cargo data and high-risk containers are identified by the Nation Targeting Center (NTC) in Virginia. The identified high-risk containers are tested for radiation by Non-Intrusive Inspection (NII) scanning in the foreign ports. CBP personnel located in the host nation ports along with the host nation law enforcement agencies evaluate the results. If the results are abnormal, the U.S. and host nation agents conduct a physical inspection of the container before it is loaded on a U.S. bound ship. The Container Security Initiative is currently operational in 58 ports in 30 countries around the world. This accounts for 80% of incoming cargo flowing into the U.S. Approximately 1% of the cargo passing through CSI-participating nations is scanned using radiation detection technology and NII scanning before being loaded and shipped to the U.S.[8]

Non-Intrusive Inspection (NII) Technology is equipment that enables CBP to detect contraband and materials that pose potential nuclear and radiological threats. The technology includes large X-ray and Gamma-ray imaging systems, as well as portable and hand held devices. More specifically, this includes, Radiation Portal Monitors (RPM), Radiation Isotopes Identification Devices (RIID), and Personal Radiation Detectors (PRD).[9]

Upon initial viewing 1% may not appear very effective and may seem to put the homeland in danger; however, the SAFE Port Act requires that 100% of cargo containers passing through U.S. POEs be scanned for radioactive material prior to being released from port. This is accomplished through choke points where all cargo is scanned with drive-through portals at U.S. ports. The radiation detection portals only need a few seconds per container to be effective. If a monitor is triggered, further tests with other technology or physical inspection are conducted.

After being identified, the cargo is either released or the radioactive material is removed and further investigation into the shipper is conducted.[10]

[8] CBP Office of Congressional Affairs, August 23, 2012.

[9] U.S. Customs and Border Protection, Fact Sheet, Non-Intrusive Inspection (NII) Technology.

[10] *Congressional Research Service, U.S. Customs and Border Protection: Trade Facilitation, Enforcement, and Security, by the Congressional Research Service,* March 2013 (Washington, DC: Government Printing Office, 2013), 28-40. CBP Office of Congressional Affairs, August 23, 2012.

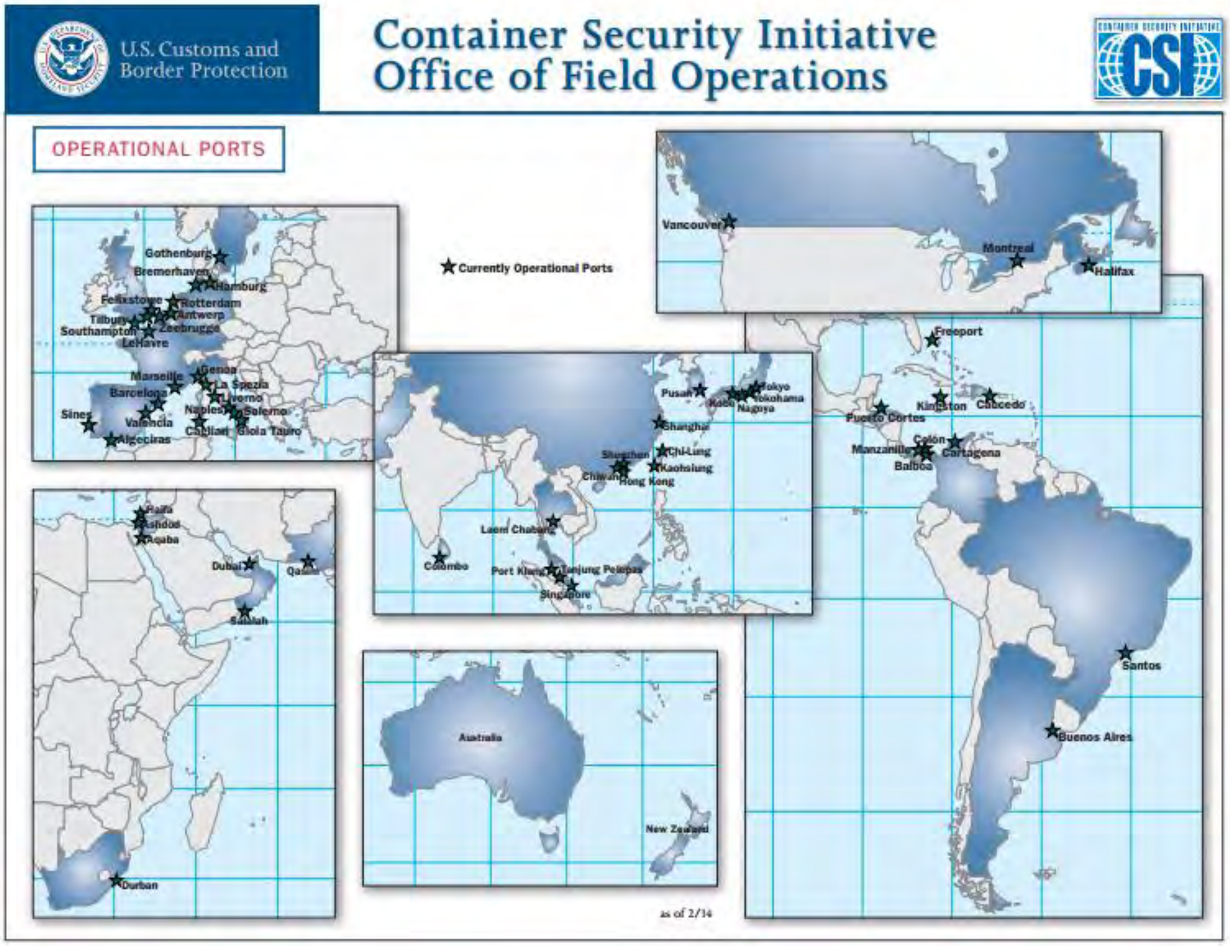


FIGURE 3.[11]

## Advise and Train

### CBP Attachés

Custom and Border Protection has also included CBP Attachés and International advisors in multiple countries around the world to increase the layered approach and to assist our international partners in capacity building programs. Attachés are posted in U.S. embassies and consulates in foreign host nations and work closely with U.S. partners and with the host nation government entities. CBP personnel work closely with U.S. investigative and intelligence

[11] Ibid. U.S. Customs and Border Protection.

personnel and advise the U.S. Ambassador and agencies of CBP programs and capabilities. These attachés assist in bridging the gap between the U.S. government and host nation governments in the previous mentioned programs in which necessitate host nation cooperation. International advisors typically are embedded with U.S. Department of Defense (DOD), other U.S. government agencies, or with the host nation border agencies. The advisors serve as consultants and trainers on international migration issues, infrastructure modernization, contraband detection, and interdiction. These operational relationships with the interagency and international partnerships are vital to the overseas footprint and effectiveness for U.S. and host nation security.[12]

### International Advisors

The U.S. military and government civilians are often tasked with providing stability operations to countries with which the U.S. has strategic relationships or that have asked for assistance. Local police play a unique role in the reconstruction of a democratic government. Foreign militaries can suppress violence and battle crime, but it is better left to law enforcement professionals. Local law enforcement can win the allegiance of the population on behalf of the local government and bring stability back to a region. The professional manner of the local police reflects the character and capacity of the government that is being reformed and reconstructed. Therefore, the police can provide crucial information when dealing with violent political factions and demonstrate to the local populace that the government is worth supporting.

[12] "The Outer Ring of Border Security: DHS's International Security Programs." *States News Service*, 2015.

Secondly, they provide security for the citizens of that country. If the local populace does not feel secure, education, employment, and economic development are in jeopardy.[13]

U.S. Customs and Border Protection agents are deployed to countries on six of the seven continents, excluding Antarctica, to provide training and technical advice to foreign host nations. The role of the adviser can range from advising General David Petraeus in Afghanistan on how best to secure the Afghanistan/Pakistan International border; to providing tracking skills to Federal Park Rangers in Kenya to combat poaching; to technical assistance on safeguarding containers with Non-Intrusive Inspection equipment in Spain. CBP personnel are deployed all over the world for differing reasons and deployment durations. However, they all offer a very valuable service to the host nation country, enable CBP to expand its ring of influence, and provide added security for the homeland.

[13] David H. Bayley and Robert Perito, *The police in war: fighting insurgency, terrorism, and violent crime*. (Boulder: Lynne Rienner Publishers, 210), 150.

# Chapter 4

## Challenges

Any type of operation or overseas deployment has a cost-benefit analysis and naysayers who think that operation is too expensive or not effective enough for continued use. As briefly highlighted in Chapter Two, there are a number of counter arguments as to why CBP should not be deployed overseas and should remain in the homeland. Budgetary concerns, cultural issues, operational effectiveness, and complexity of the problem (as seen below) are the major issues that have been offered as to why CBP's footprint should not be expanded. Because the Department of Defense is a much larger organization and has more background with such issues, the parallels, as mentioned earlier in this paper, will be analyzed along with other references for a defensible counter argument.

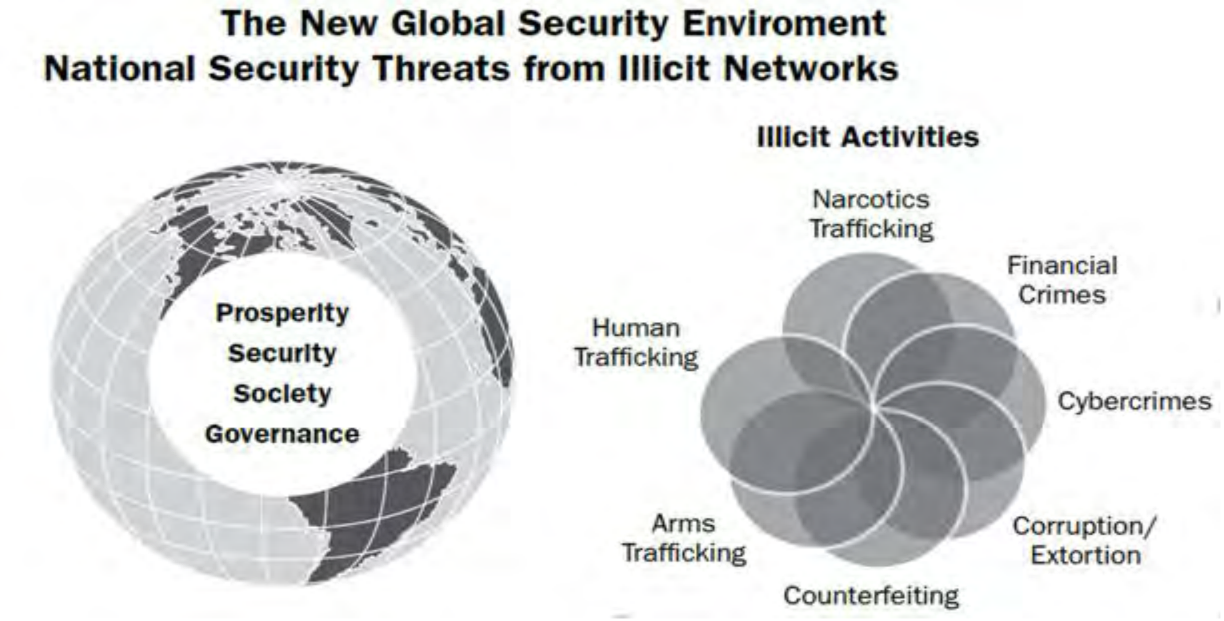


FIGURE 4. [1]

[1] Michael Miklaucic, and Moises Naim. "The Criminal State," in *Convergence: Illicit Networks and National Security in the Age of Globalization (*Washington, D.C.: National Defense University Press, 2013), 150-151.

Budget Constraints

As with any operation, agency, or department, one's budget is what drives the ability to complete the mission. In the last 15 years, the U.S. has been involved in two very costly wars in Afghanistan and Iraq costing roughly $ 4.8 trillion. This figure includes: direct Congressional war appropriations; war related increases to the Pentagon base budget; veteran care and disability; increase in the homeland security budget; interest payments on direct war borrowing; foreign assistance spending; and estimated future obligations for veterans' care.[2] Although CBP's overall budget is only a fraction of that, it still affects the overall budget of the U.S. Government and contributes to the budget constraints on all departments and agencies. The budget of CBP in 1995 was $1.4 billion. After the attacks of 9/11, by 2006, the budget had almost quadrupled to $4.7 billion.[3] For 2017, the proposed CBP budget is $13.9 billion. This is a considerable increase in funding for manpower, technology, and infrastructure. Within that number are the numerous personnel and operating costs needed to train, house, and protect the agents that are stationed overseas.

On May 29, 2015, Department of Homeland Security (DHS) Secretary Jeh Johnson announced DHS's intention to enter into negotiations to expand air pre-clearance to ten new foreign airports, located in nine separate countries. In 2014, nearly 20 million passengers traveled from these ten international airport to the U.S. As discussed earlier, preclearance allows for the complete inspection of the individual before boarding the flight. More than 16 million individuals traveled through one of CBP's pre-clearance locations in Canada, Ireland, the

[2] Watson Institute for International and Public Affairs, "*Costs of War,*" Brown University, http://watson.brown.edu/costsofwar/figures/2016/us-budgetary-costs-wars-through-2016-479-trillion-and-counting (accessed December 28, 2016).
[3] Harold Kennedy, "Border Security," *National Defense*, Vol. 91, Issue 632, (July 2006): 47.

Caribbean, or the United Arab Emirates in FY 2015. CBP's goal by 2024 is to process 33 percent of the U.S. bound air travelers abroad, before they ever board an airplane. The Consolidated Appropriations Act of 2016 (Pub. L. No. 114-113) provided the up-front appropriations that CBP may use to cover costs of pre-clearance operations until reimbursements are collected. The intent of this program is for reimbursements to help fund the cost of the program. These reimbursement come from airport operators. As of FY 2017, CBP has not collected any of the reimbursements from foreign airports. This, of course, may change in the future, but with the perception of the deep pockets of the U.S. government, foreign airports have been reluctant to pay to have U.S. CBP agents in their airports conducting security checks on the their citizens before departing. At issues is whether those agents and funding for them would be better utilized in the U.S. where there is positive control and better access to needed technology to conduct 100% checks. Having an effective number of agents deployed internationally performs a number of deterrence phases to the security of the homeland and increases the security of the host nation partners. The U.S. funds the CBP officers and the host nation covers the pre-clearance operations. With increased security, lower wait times for passengers, and increased throughput of cargo, the host nation is more effective and efficient. Ultimately, this program has proven to be successful and should remain, however, efforts must be increased to collect reimbursements.

### Cultural Issues

Cultural issues that can provide obstacles to overseas deployment and combatting transnational criminal organizations are both external (host nation) and internal to the U.S. agencies countering these organizations. Networks of criminal organizations, terrorists, and smugglers are not a concept new to the 21st century; they are as old as man himself. The new and emerging issues with these networks are their ability to globalize and the U.S. ability to counteract them. The methods for smuggling are no longer simple trails with donkeys loaded with illegal goods. Globalization has increased the quantity and speed at which items can move. Because of the international networks and number of players there is a lack of data regarding the operations and structures of these networks. If data is available, the networks are so complex that the computer models, testing, and tools do not have the technical capability to interpret them. This conceptual underdevelopment of the study of illicit networks and organizations is one of the core problems and provides for an enormous vacuum to counteract them.

Sociologists, criminologists, and anthropologist all perceive transnational criminal organizations as differing phenomena. Sociologist view these organizations from a model based on their discipline, emphasizing the dynamics of collective human behavior. Criminologists tend to view transnational crime as an extension of individual criminality, best left to law enforcement agencies. Anthropologists, political scientists, and international relations specialists perceive the phenomenon through their colored lenses, which are also conflicting. These academic conflicts inevitably lead to conceptual confusion, competing models, and interdisciplinary competition for a definition of what transnational criminal organization are and how to combat them. [4]

This academic confusion also bleeds over into the operational aspects of combatting international transnational criminal organizations. Lawyers will see them differently from law enforcement professional, who will see them differently from Department of Defense personnel. All have a vested interest in their niches and agendas. The number of agencies that are attempting to combat transnational crime are as numerous and varied as the networks they are

[4] Ibid. Miklaucic, and Naim. 150-151.

attacking. Each organization has its own organizational culture, methods, authorities, jurisdictions, and idiosyncrasies. Just a few of the organizations who are involved in the effort to counter the illicit networks are: the State Department, Department of Defense, Department of Justice, Department of Homeland Security, and the Treasury Department. These parent organizations are further broken down into the Federal Bureau of Investigation; the Drug Enforcement Administration; the Bureau of Alcohol, Tobacco, Firearms, and Explosives; and the U.S. Customs and Border Protection. To further complicate issues, various intelligence agencies are involved, including the Central Intelligence Agency, Defense Intelligence Agency, and each of the DHS agency intelligence offices. Law enforcement organizations understand their role as building criminal cases and prosecuting the individual or organization in a court of law. Whereas military organizations tend to view the challenges in terms of battle campaigns and strikes. The problem of information sharing between organizations is also extremely difficult because of classifications and internal relationships. The differences that have been discussed above are just a few of the problems preventing effective cooperation and the ability to be successful against the transnational criminal networks.[5]

Even more complicated can be the relationship between host nation countries with respect to each other and with the United States. These aforementioned conceptual seams create differing perceptions of illicit networks and illicit commerce within multilateral and bilateral efforts to combat transnational crime. Some nation-states view narcotic trafficking as a demand problem, while others view it as a supply problem; counterfeiting can be seen as a violation of international law or, it may be viewed as a jobs program and method to inject money into the system. National borders are what create price differentiation and supply and demand issues that

[5] Ibid., 150.

drive the profits of illegal commerce. Borders also provide a safe haven for criminals, terrorists, and illicit networks to hide within. The laws of the nation-state, differences in sovereignty, and border seams allow for the constant jumping back and forth between countries. This creates jurisdictional nightmares for governmental agencies working to combat illegal activities. So while borders are very confining and necessary for national sovereignty, they allow for traffickers to justify their existence, protect them, make their way of life possible, and allow their business to be profitable.[6]

### Operational Effectiveness

There are three conceptual delusions regarding transnational criminal networks that influence the way nation-states, law enforcement, defense departments, and civilians combat them. The first is the attitude that crime is crime, and it has been around since the beginning of time, and there is nothing new out there. This is the wrong way to view the problem. The velocity and magnitude of illicit commerce today are unprecedented, representing between 2 to 25 percent of global products.[7] That amount of illicit goods greatly contributes to a culture of corruption, physical threats against nation states, and the loss of billions of dollars in legal taxes and tariffs. Secondly, illicit networks and transnational crime are often viewed as just about crime and criminals. If the problem is dealt with in a traditional way, with the typical institutions of law enforcement, courts, and jails, the problem will not be solved. The challenge is with the public institutions, and integrity of public administration and their ability to provide incentives and reinforce the value of service to the state. This needs to be a grassroots effort that starts in the schools, churches, homes, and communities through media and with the application of

[6] Ibid., 151-152.
[7] Ibid., 152.

incentives and disincentives. Lastly, the individuals involved cannot be regarded as criminals and deviants. Cesare Lombroso, a 1900th century Italian criminologist, argued that criminal nature is inherited and represents a regression from normal human development. His theory of anthropological criminology does not apply and these criminal individuals are only a product of their situation.[8] Just because one is a criminal does not necessarily mean he is a deviant. Approximately 8 to 10 percent of China's gross domestic product is associated with the manufacturing and sale of counterfeit goods. Even more alarming, sixty percent of Afghanistan's gross national product comes from the cultivation, production, and distribution of the poppy.[9] Utilizing these two examples and noting the number of people who are involved in the transnational networks, are they guilty of breaking criminal statutes and deviants or just trying to provide for their families? This only adds to the complexity of the problem, who to arrest, and how to attack it.

As discussed earlier in this paper, deterrence is the primary method CBP utilizes to combat transnational crime. By utilizing multiple checks and layered security, the bad actors know it is almost impossible to avoid detection through the common channels that they would commonly move people or illegal goods. For this reason they must utilize other, more expensive, dangerous paths. These commodity chains often span significant geographic areas and require multiple steps, payments, and individuals to be successful. Those who often move the products do not have direct access to money laundering, hawala networks, or transportation networks for the profits of these commodities. Payments are made with cash, weapons, drugs,

[8] David Horn, *The Criminal Body: Lombroso and the Anatomy of Deviance, (New York: Routledge 2006),* 18.
[9] Ibid., Miklaucic, and Naim, 150.

chemicals or other materials that are deemed valuable to the network.[10] This creates huge losses and complexities in the chain and makes the transportation of illicit goods and people very difficult.

The true issue with deterrence operations, whether in Department of Defense or U.S. Customs and Border Protection operations, is that there is no true way of knowing if deterrence is effective. The previous paragraphs illustrate how deterrence operations are intended to work and cause discomfort and confusion for transnational criminal organizations. However, there are no measures of effectiveness on the quantity of an illegal good or the number of people that are still making it into the U.S. without inspection. At best, it is estimated that only one third of all illegal aliens and illicit material are being interdicted. Some argue that CBP personnel and resources would be better allocated in the homeland where interdictions and arrests can be better measured and personnel are playing on their home turf.

Measuring direct and indirect impacts to transnational crimes require a great number of assumptions, data, and models that cannot totally be understood because of the size and complexity. However, using the United Nations Office of Drugs and Crime (UNODC's) model for impact of illegal markets it is estimated that the total amount for illegal drugs, human trafficking, excised goods, environmental crimes, and counterfeits can reach the $1.5 trillion in direct and indirect effect on society.[11] With those facts it is important for CBP to do everything

[10] Douglas Farah, "Fixers, Super Fixers, and Shadow Facilitator: How Networks Connect," in *Convergence: Illicit Networks and National Security in the Age of Globalization, (*Washington, D.C.: National Defense University Press, 2013), 75-76.

[11] Justin Picard, *"Can We Estimate the Global Scale and Impact of Illicit Trade"* in *Convergence: Illicit Networks and National Security in the Age of Globalization, (*Washington, D.C.: National Defense University Press, 2013), 57.

in its power to combat these issues. Providing deterrence in foreign countries to increase the chance of seizures and the arrest of individuals is well worth the effort, risk, and funding.

# Chapter 5

## Recommendations and Conclusion

### Recommendations

This paper has outlined the benefits of CBP's expansion overseas and will provide recommendations on how that expansion can continue and improve both the host nation and the U.S.'s national security. The first recommendation is to continue the assessment of the countries in which CBP is invested. The Assistant Commissioner of International Affairs, Mark R. Koumans, twice a year has either a face-to-face or a secure video teleconference meeting with all of the CBP attachés worldwide to discuss the status of CBP, the impact it is having in those host nations, and if continued engagement is needed. These semi-annual assessments ensure that CBP's personnel and budget are utilized wisely and effectively. The agency and the attachés are flexible and adaptable enough that if they need to return to the U.S. it can be accomplished rather quickly.

Second, CBP should continue and expand its overseas short term deployment to countries that request assistance. The Border Patrol Special Operations Group needs to continue to send teams to countries that need assessments. Short term deployment teams are able to assess what a country's border enforcement capability and capacities are and how to improve them. The gaps could be in hiring, initial training, leadership, and or technology and infrastructure. Although most countries do not have the financial abilities to train, equip, and provide infrastructure similar to the U.S., small improvements in training, tactics, and procedures can greatly influence one's ability to be more effective.

Lastly, the Office of Field Operations needs to engage the CBP Office of Trade to continue and expand their international operations and advisement. Enforcement is only half of the CBP mission, the other half is the facilitation of trade and travel. CBP personnel need to engage individuals in transit to the U.S., container security initiatives, and trade procedures. The U.S., if needed, could lock the border down so no one could enter or depart. This idea, however, is not conducive to the American way of life both for personal travel and for the goods the U.S. imports and exports. There needs to be a balance between travel and trade and enforcement and interdiction.

## Conclusion

This paper has outlined the events that led to the formation of the Department of Homeland Security and U.S. Customs and Border Protection, the damage that transnational criminal organizations can do to U.S. national interests and security, how CBP's expanding footprint is assisting with the security of the homeland, the challenges and counter-argument to CBP's expansion, and finally recommendations for expansion of overseas operations to further the efficiency and effectiveness on the CBP mission. Both sides of the original thesis question: Bigfoot or big mistake: Is CBP's expanding footprint helping or hurting homeland security? have been addressed. CBP International Affairs is only a small part of DHS and an even smaller part of the giant U.S. government. However small of a portion of the government it is, CBP International Affairs plays a major role in the whole of government approach to securing the U.S.'s national interests and security. It is vital to national security that CBP continue to be deployed and engaged overseas.

## BIBLIOGRAPHY:

Bayley, David H., and Robert Perito. *The police in war: fighting insurgency, terrorism, and violent crime*. Boulder: Lynne Rienner Publishers, 2010.

Bonner, Robert C. "Securing the transnational movement of trade and people in the era of global terrorism." *Strategic Insights Series,* June 2006, 1-20.

Boot, Max. *Invisible Armies: an epic history of guerrilla warfare from ancient times to the present*. New York: Liveright Pub. Corporation, 2013.

Congressional Research Service. *Border Security: Immigration Enforcement between Ports of Entry, by the Congressional Research Service,* April 2016. Senate Print. Washington, DC: Government Printing Office, 2016.

______. *Terrorism and Transnational Crime: Foreign Policy Issues for Congress, by the Congressional Research Service,* June 2013. Senate Print. Washington, DC: Government Printing Office, 2013.

______. *U.S. Customs and Border Protection: Trade Facilitation, Enforcement, and Security, by the Congressional Research Service,* March 2013. Senate Print. Washington, DC: Government Printing Office, 2013.

Farah, Douglas. "Fixers, Super Fixers, and Shadow Facilitator: How Networks Connect," in *Convergence: Illicit Networks and National Security in the Age of Globalization,* 75-95. Washington, D.C.: National Defense University Press, 2013.

Horn, David. *The Criminal Body: Lombroso and the Anatomy of Deviance*. New York: Routledge, 2006.

Kennedy, Harold. "Border Security." *National Defense*. July 2006, Vol. 91 Issue 632, p 46-47.

Kilcullen, David. *Counterinsurgency*. Oxford; New York: Oxford University Press, 2010.

______. *Out of the Mountains: the coming age of the urban guerrilla*. Oxford; New York, NY: Oxford University Press, 2013.

Miklaucic, Michael and Moises Naim. "The Criminal State," *Convergence: Illicit Networks and National Security in the Age of Globalization,"* 149-170. Washington, D.C.: National Defense University Press, 2013.

Novakoff, Renee. "Transnational Organized Crime." *PRISM Security Studies Journal* 5, no. 4 (December 2014): 134-149.

Quadrennial Defense Review 2014. Department of Defense. Washington, DC: Government Printing Office. February 2014.

Pawlak, Patryk. "Transatlantic homeland security cooperation: the promise of new modes of governance in global affairs." *Journal of Transatlantic Studies (Routledge)* 8, no. 2 (Summer 2010): 139-157.

Peinhardt, Clint, and Todd Sandler. *Transnational Cooperation: An Issue-Based Approach*. New York: Oxford University Press, 2015.

Peters, Gerhard and John T. Woolley, "Summary of Smart Border Action Plan Status." *The American Presidency Project,* September 9, 2002. http://www.presidency.ucsb.edu/ws/?pid=79762Online by Gerhard Peters and John T. Woolley (accessed December 27, 2016).

Picard, Justin. "Can We Estimate the Global Scale and Impact of Illicit Trade," In *Convergence: Illicit Networks and National Security in the Age of Globalization,* 37-59. Washington, D.C.: National Defense University Press, 2013.

Restrepo, Daniel A. "Individual Based, Cross Border Litigation: A National Security Practitioner's Perspective." *University of Pennsylvania Journal of International Law.* 2013, Vol. 34 Issue 4, p 743-753.

U. S. Border Patrol National Strategy 2012-2016, The Mission: Protect America. Washington DC: Government Printing Office, January 2012.

U.S. Congress, House, Committee on Homeland Security, Reorganization Plan Modification for the Department of Homeland Security, Communication from the President of the United States, House Document 108-32, 108th Cong., 1st sess., February 3, 2003.

______. Written Testimony of CBP Office of Field Operations Deputy Assistant John Wagner for House Committee on Homeland Security, Subcommittee on Border and Maritime Security Hearing Titled' The Outer Ring of Border Security: DHS's International Security Programs. *States News Service*, 2015. *Biography in Context*.

______. Written Testimony of CBP Commissioner R. Gil Kerlikowski for a House Committee on Appropriations, Subcommittee on Homeland Security Hearing on the U.S. Customs and Border Protection's FY 2017 Budget Request. *States News Service*, 2016. *Biography in Context*.

U. S. Customs and Border Protection. "About CBP." https://www.cbp.gov/about.

______. Fact Sheet, Non-Intrusive Inspection (NII) Technology, 2013.

______. Officers Working at the Aruba Pre-Clearance Facility Intercepted Nearly Five Pounds of Cocaine Concealed in a Travelers Luggage Liner. *States News Service*, 2016. *Biography in Context*.

U.S. Customs and Border Protection. *Vision and Strategy 2020, Strategic Plan*. Washington, DC: Government Printing Office. March 2016.

U.S. Department of Homeland Security. "About DHS." https://www.dhs.gov/sites/default/files/publications/Department%20Org%20Chart_1.pdf.

U.S. President. *National Security Strategy.* Washington DC: Government Printing Office, February 2015.

______. *Strategy to Combat Transnational Organized Crime. Addressing Converging Threats to National Security*. Washington DC: Government Printing Office, July 2011.

Watson Institute for International and Public Affairs, "*Costs of War,*" Brown University, http://watson.brown.edu/costsofwar/figures/2016/us-budgetary-costs-wars-through-2016-479-trillion-and-counting (accessed December 28, 2016).

# VITA

Mr. Christopher M. Seiler, (DHS/CBP) is the Patrol Agent in Charge serving in the U.S. Border Patrol. He began his career in 2001 in San Diego Sector. In 2005 he became a member of the Border Patrol Tactical Unit (BORTAC) and served on numerous overseas assignments, including Iraq. In 2008 he was promoted to Supervisory Border Patrol Agent in Imperial Beach, CA. He became an Assistant Attaché in Kabul, Afghanistan for CBP International Affairs from 2011-2013. Following his service as an attaché he was promoted to Operations Officer at the U.S. Border Patrol Headquarters in Washington, D.C., where he was later promoted to Assistant Chief in 2013. His most recent command is the Patrol Agent in Charge of the Special Operations Detachment in McAllen, TX. Mr. Seiler has a B.S. in Criminal Justice and a Master's Certificate in Advance International Affairs.

From: (b)(6);(b)(7)(C)

To: (b)(6);(b)(7)(C)

Cc: (b)(6);(b)(7)(C)

Bcc:
Subject: RE: Final Cleared version "Biometric Breakthrough: How CBP is meeting its Mandate and Keeping America Safe" -- Frontline Magazine
Date: Sat Nov 04 2017 09:01:54 EDT
Attachments: Frontline - Vol9 Iss3 - 1104 - Biometrics.pdf

Good morning everyone,

The attached PDF is the Biometrics section of the magazine with the updated text in the layout.

(b)(6);(b)(7)(C) I sent you a copy of the full magazine proof in a separate email in case you need to share with anyone.

(b)(6);(b)(7)(C)

Visual Information Specialist / Public Affairs Officer

U.S. Customs and Border Protection

Office of Public Affairs

From: (b)(6);(b)(7)(C)
Sent: Friday, November 03, 2017 5:03 PM
To: (b)(6);(b)(7)(C) >
Cc: (b)(6);(b)(7)(C)
Subject: Final Cleared version "Biometric Breakthrough: How CBP is meeting its Mandate and Keeping America Safe" -- Frontline Magazine
Importance: High

Hi (b)(6);(b)(7)(C)

As we discussed earlier, I met with (b)(6);(b)(7)(C) this afternoon and went over the suggested edits from the Front Office that pertained to him. He has cleared the attached version. So we are ready to move forward.

Also as we discussed, when you send the final layout to (b)(6);(b)(7)(C) please let me take a look at the biometric articles, so I can proof them one more time before you send everything to the printer.

Thanks so much! Have a great weekend and please tell your family I said hello! :-)

Take care,

(b)(6);(b)(7)(C)

P.S. I did not attach the two biometric side stories because, as I mentioned, the Front Office cleared them as is.

(b)(6);(b)(7)(C)

Writer/Editor

Communication and Outreach Division

Office of Public Affairs

U.S. Customs and Border Protection

Ph: (b)(6);(b)(7)(C)

Email: (b)(6);(b)(7)(C)

www.cbp.gov

From: (b)(6);(b)(7)(C) [redacted]

To: (b)(6);(b)(7)(C) [redacted]

Cc: (b)(6);(b)(7)(C) (b)(6);(b)(7)(C) [redacted]

Bcc:
Subject: Frontline Proof - 10-06-2017
Date: Fri Oct 06 2017 10:52:22 EDT
Attachments: Frontline - Vol9 Iss3 - 1006.pdf

(b)(6);
(b)(7)

Not trying to bother you on your vacation, but I wanted to give you an opportunity to take a look at the current Frontline proof. I'll be delivering a proof to AC Friel on Monday.

Enjoy the sunshine,

(b)(6);
(b)(7)

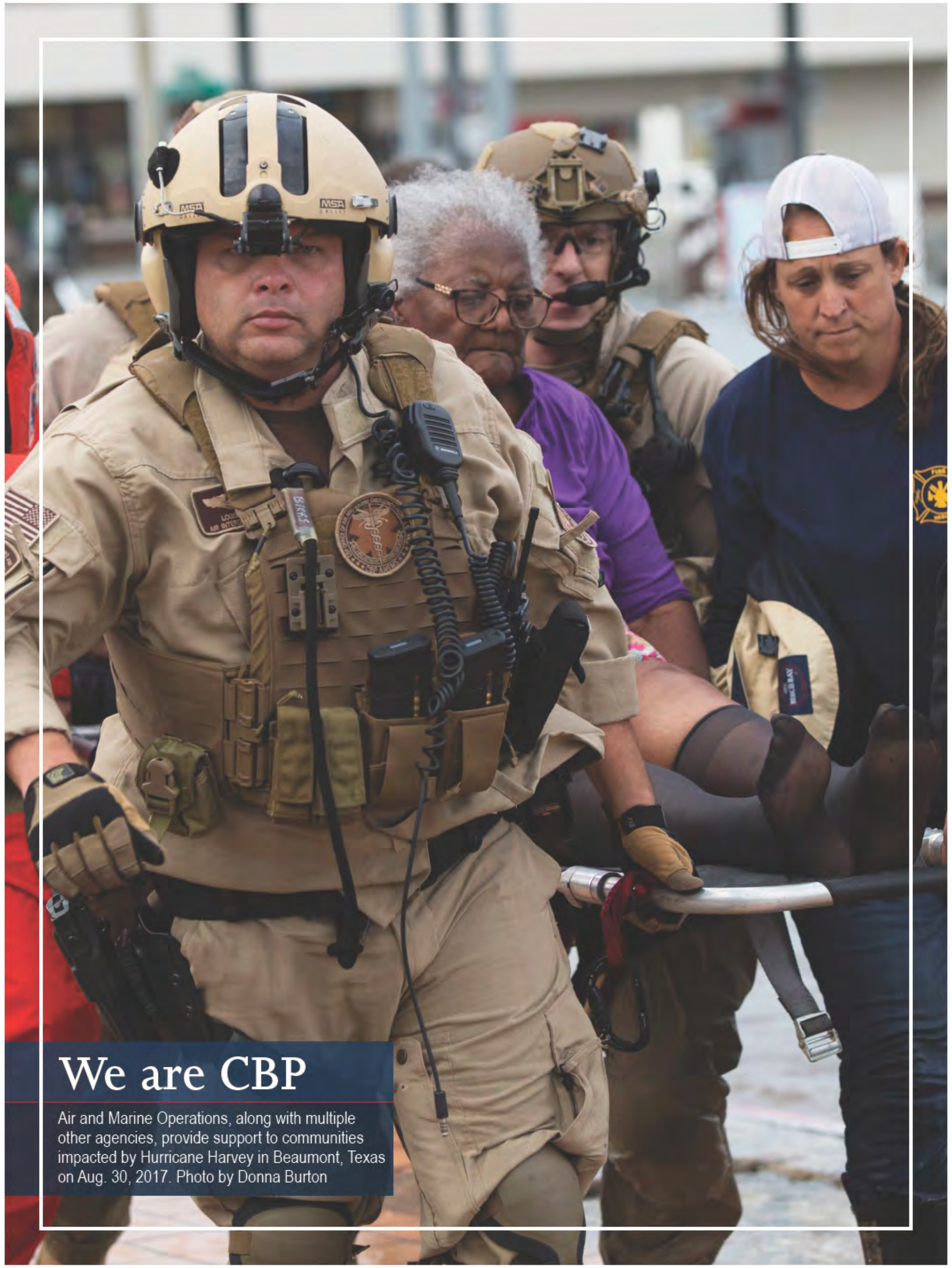
# FRONTLINE

U.S. CUSTOMS AND BORDER PROTECTION

VOL 9 • ISSUE 3

## BIOMETRIC BREAKTHROUGH

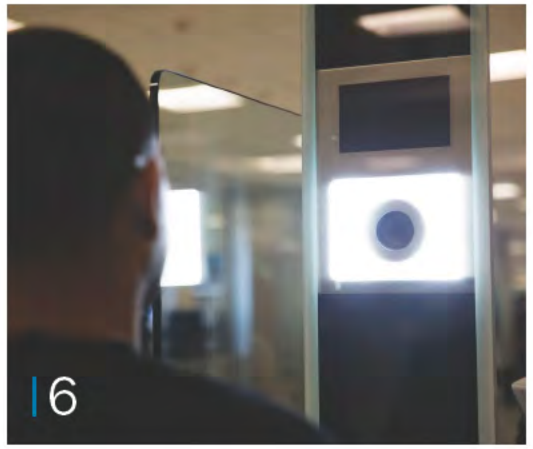
HOW CBP IS MEETING ITS MANDATE AND KEEPING AMERICA SAFE

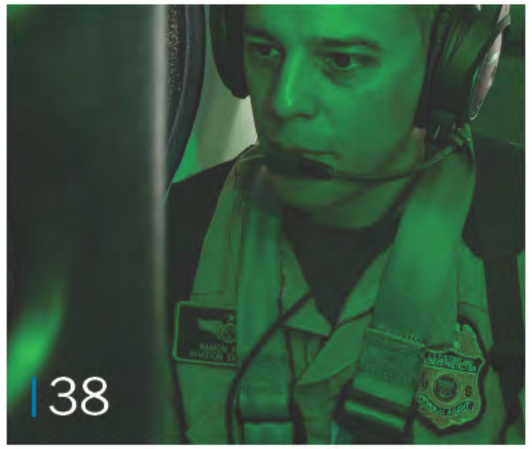


## We are CBP

Air and Marine Operations, along with multiple other agencies, provide support to communities impacted by Hurricane Harvey in Beaumont, Texas on Aug. 30, 2017. Photo by Donna Burton

# Contents





COVER

Photo and composite by Ozzy Trevino

This example of facial recognition technology does not reflect the specific hardware and software used by carriers.

FRONTLINE

SECRETARY OF HOMELAND SECURITY (ACTING)
Elaine Duke

COMMISSIONER (ACTING),
U.S. CUSTOMS AND BORDER PROTECTION
Kevin K. McAleenan

ASSISTANT COMMISSIONER (ACTING),
OFFICE OF PUBLIC AFFAIRS
Michael J. Friel

EDITOR
Laurel Smith

MANAGING EDITOR
Jason McCammack

PRODUCTION MANAGER
Tracie Parker

STAFF WRITERS
Paul Koscak, Marcy Mason

STAFF PHOTOGRAPHERS
Donna Burton, Glenn Fawcett

ART & DESIGN DIRECTOR
Ozzy Trevino

The Secretary of Homeland Security has determined that publication of this periodical is necessary in the transaction of public business by CBP.

To contact Frontline editors with messages, contributions, or delivery concerns, email: **frontline@cbp.dhs.gov**

U.S. Customs and
Border Protection

Photo by Artens/Shutterstock.com

# BIOMETRIC BREAKTHROUGH

## HOW CBP IS MEETING ITS MANDATE AND KEEPING AMERICA SAFE

By Marcy Mason

It's 7:45 on a Wednesday morning in May at Hartsfield-Jackson Atlanta International Airport and passengers are boarding Delta Air Lines flight 334 to Mexico City. One by one the passengers scan their boarding passes and approach a camera that's set up on a jetway where they have their pictures taken before they board the flight.

The photos are being matched through biometric facial recognition technology to photos that were previously taken of the passengers for their passports, visas, or other government documentation. All is moving smoothly until the U.S. Customs and Border Protection officers assisting the passengers are alerted that they need to check one of the travelers.

It's a 28-year old woman, a Mexican national with a Mexican passport. The biometric system alerted the officers because when preflight information was gathered on the woman, no historical photos to match against her could be found.

A CBP officer took the woman aside and looked at her passport. No visa was attached and the woman didn't have a green card to prove she was a lawful permanent resident. Upon further questioning, the woman admitted that four years ago, she had come into the country illegally.

Using a specially designed, CBP biometric mobile device, the officer took fingerprints of the woman's two index fingers. "This was the first time that we had captured this individual's biometrics, her unique physical traits," said Bianca Frazier, a CBP enforcement officer at the Atlanta Airport. "We didn't have her biometrics because we had never encountered her before."

As early as 2002, shortly after the worst terrorist attack in U.S. history, legislation was passed requiring the Department of State and the Department of Homeland Security to use biometric technology to issue visas and screen non-U.S. citizens entering the U.S. Then in 2004, more legislation was passed, authorizing DHS to collect biometric data from non-U.S. citizens exiting the country.

According to Frazier, finding people who have entered the country illegally is common. Since June 2016, when CBP and Delta Air Lines launched a pilot program to test CBP's biometric facial recognition exit technology, passengers like the young Mexican woman have been found daily. "She was typical of the people who have entered without inspection," said Frazier. "Most days we find a minimum of two or three undocumented people, but sometimes we find as many as eight to 10 boarding a flight."

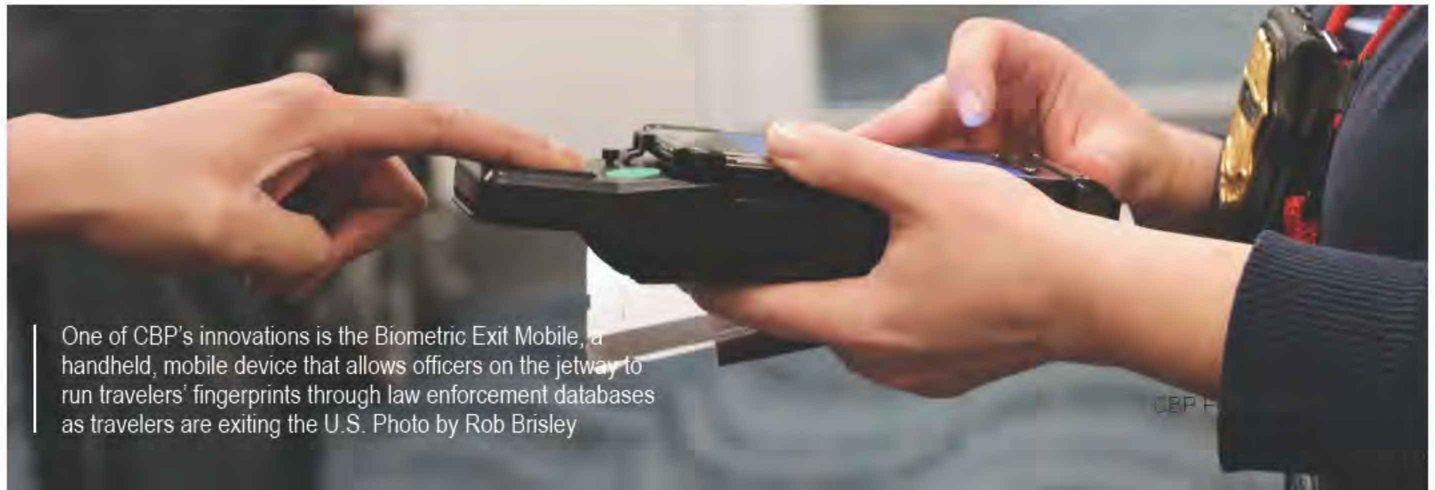
Ultimately, the woman was allowed to board the flight, but when Frazier used CBP's mobile device to take her fingerprints, it created a fingerprint identification number that is specifically tied to the woman. In the future, if she applies for a visa to return to the U.S. or is encountered crossing the border illegally, an alert will be triggered, indicating that the woman had previously entered the U.S. illegally and is on a lookout list. Additionally, when Frazier processed the traveler, the device automatically created a biometric exit record confirming that the woman left the country.

For more than a decade, the U.S. government has been struggling to find a way to develop a practical and cost-effective biometric entry/exit system that fulfills a congressional mandate to keep America safe. CBP has partnered with the U.S. air travel industry to meet that goal and is implementing innovative ways of using biometric technology to provide better enforcement and a better experience for travelers.

## Biometric challenge

By 2013, when CBP assumed responsibility for designing and implementing a system that could biometrically track travelers exiting the U.S., the government had been wrestling with the challenge for years. Technology was part of the problem, but how to integrate that technology into the existing infrastructure at airports without driving up costs and negatively impacting airport and airline operations was a conundrum.

CBP had been working with the airlines to track travelers entering and exiting the country since the mid-1990s, using travelers' biographic



One of CBP's innovations is the Biometric Exit Mobile, a handheld, mobile device that allows officers on the jetway to run travelers' fingerprints through law enforcement databases as travelers are exiting the U.S. Photo by Rob Brisley information— date of birth, passport number, document number,  country of citizenship, etc. "The airlines sent us the manifest information in advance of the flight's departure," said John Wagner, deputy executive assistant commissioner of CBP's Office of Field Operations. "We did law enforcement work based on that data."

But then, after September 11, biographic information wasn't enough. To increase security, Congress passed legislation that added biometric requirements for tracking travelers. "Inbound passengers were easier to track because we already had a process," said Wagner. "When travelers come off of an international flight, they are funneled through a secure pathway to the CBP inspection area. The airline transmits the biographic data to us. We verify that information when we read a traveler's passport and we make sure it's accurate. That's when we also collect fingerprints from most non-U.S. citizens."

With outbound flights, collecting passengers' biometrics is much more difficult. "We've never constrained departures to be able to do that," said Wagner. "We don't have specific departure areas for outbound flights. International flights depart from all over the airport, so it was difficult to figure out where we could collect biometrics and what technology we would use."

Added to that, CBP lacked support. "The travel industry stakeholders were vehemently opposed to any of this because they thought it would cost money and it would slow people down," said Wagner. The challenges seemed insurmountable. "We were focused on where is the magic technology that is going to make this work and address all of these concerns. No one had been able to find it because it didn't exist," he said.

## New beginning

Wagner and his team took a fresh start. They reached out to the DHS Science and Technology Directorate, the department's research and development arm, to learn more about the biometric technology that was available and which methods of collection would work best. Shortly thereafter, in 2014, a demonstration test lab was set up in Landover, Maryland. "One of the things we learned from previous pilots in airports is that airports are chaotic places. It's hard to do a really good controlled test when anything can go wrong and you don't know why. Was it because there were lots of delays? Were there weather incidents? Or did people miss their flights? Any number of factors could affect the performance of the biometric system, so we set up a test space where we could carefully control different variables to see how well our biometric concepts worked," said Arun Vemury, director of the DHS Science and Technology Directorate's Apex Air Entry/Exit Re-engineering and Port of Entry People Screening programs.

"We evaluated more than 150 different biometric devices and algorithms. We put them together in different configurations and then brought in test volunteers to actually run through the process to figure out how long it took, what kind of throughput we were able to get, how well the biometrics matched, and what their performance ultimately was," said Vemury "Over time, we brought in more than 2,000 people from 53 different countries of origin, who varied in age from 18-85. We were trying to mimic the demographics of travelers coming to the U.S."

One of the things that Vemury learned was that the algorithms used in facial recognition technology have become much more advanced. The algorithm is the formula that identifies the unique biometric features in a finger, iris, or face and then compares those points to corresponding areas in previously collected biometrics. "Because of the improvements in facial recognition technology, we can verify people's identities with facial recognition much more effectively today than we could even just two years ago," said Vemury.

After nearly two years of rigorous testing and evaluation, DHS Science and Technology gave its findings to CBP in December 2015. "We turned over all of our test reports, economic analyses, quantitative analyses, concepts of operation, and staffing estimates," said Vemury. "The last thing we wanted was to have any unanswered questions. We knew we needed a biometric process that would work."

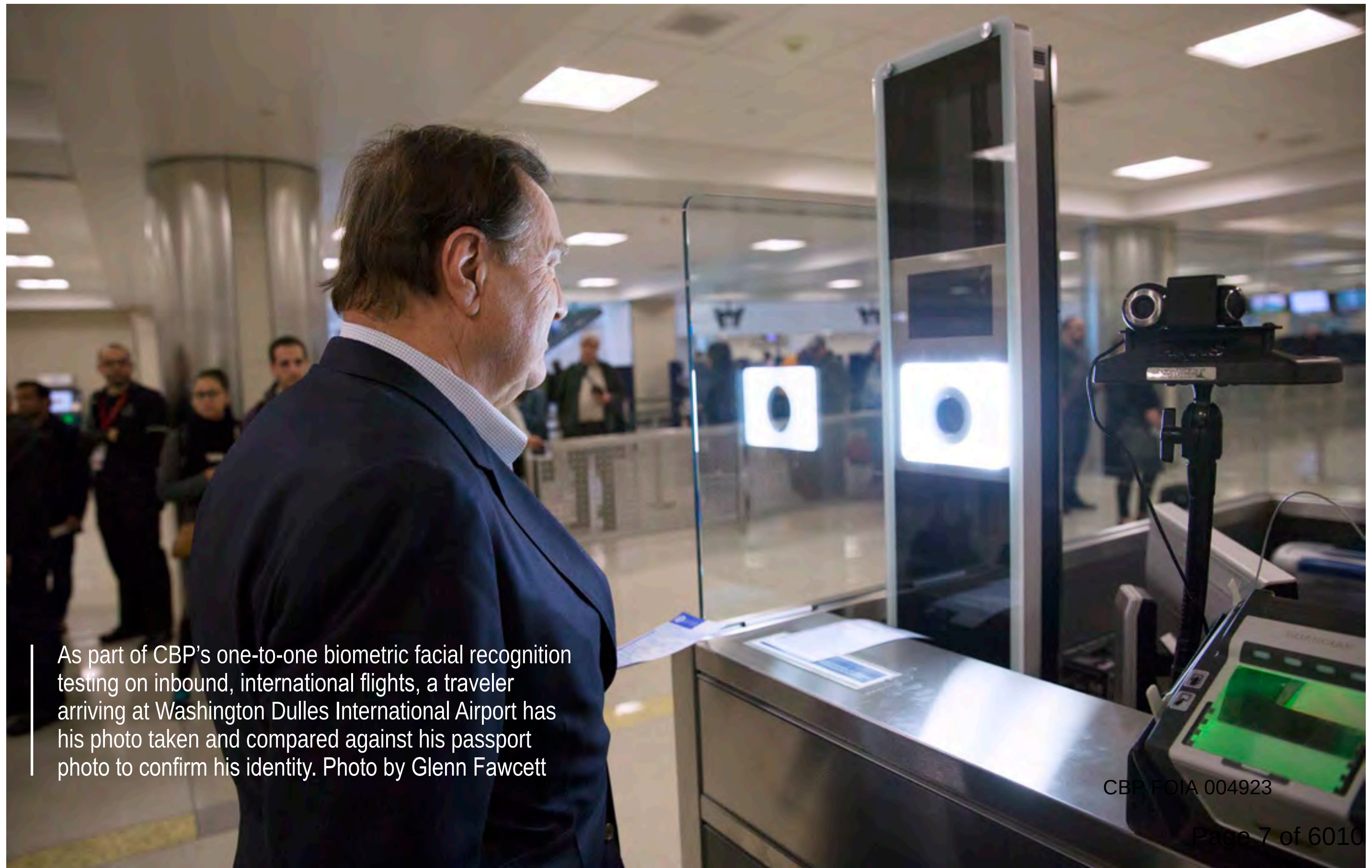
## Field testing

Concurrently, CBP was doing its own laboratory tests and conducted a series of pilots. "We ran several pilots to help us learn about the different types of biometric technology in the different environments where we work," said Wagner. For example, CBP was aware that U.S. passports were vulnerable to fraud and thought a biometric tool could help. After months of testing algorithms and cameras, CBP developed a one-to-one facial recognition technology that compared travelers against their passport photos. The pilot, which was tested on inbound flights, initially ran for two months, from March to May 2015, at Washington Dulles International Airport in Dulles, Virginia. At that point, more lab testing and analysis was done to improve the algorithm, and then a second pilot, which continues today, was set-up at Dulles and John F. Kennedy International Airport in New York City.

"The pilots showed us that the facial recognition technology was accurate," said Wagner. "We grew confident that the algorithms were good enough to use and rely on."

One of the many examples that illustrates this occurred at JFK in May 2016, when a traveler with a U.S. passport arrived on a flight from Accra, Ghana, and presented herself as a returning U.S. citizen. All of her biographical information was processed successfully, but the CBP officer who interviewed the woman had a suspicion she might be an imposter. The officer referred the traveler to a booth equipped with the facial recognition technology where her photo was taken and compared to the photo in her passport. The match score was very low and she was referred for further inspection.

The woman was fingerprinted and the officers confirmed her true identity, uncovering that she was an imposter. In actuality, the woman was a Liberian citizen who had been denied a diversity visa from a green card lottery in 2015. She admitted that she found the U.S. passport in a marketplace and didn't know the true owner. The woman was then turned over to U.S. Citizenship and Immigration Services



As part of CBP's one-to-one biometric facial recognition testing on inbound, international flights, a traveler arriving at Washington Dulles International Airport has his photo taken and compared against his passport photo to confirm his identity. Photo by Glenn Fawcett authorities and sent to a detention center to await a credible-fear hearing to determine whether she would be able to seek asylum. Without the suspicions of an astute officer and CBP's biometric technology, the woman could have entered the country through fraudulent means.

In another pilot at the land border, in Otay Mesa, California, CBP tested face and iris scans to biometrically record the entry and exit of pedestrians. "From these tests, we learned a lot about how travelers react to various biometric technologies," said Wagner.

CBP also built a handheld, mobile device that allowed officers to run fingerprints on departing travelers. "We tested the Biometric Exit Mobile in 2015 at 10 airports around the country," said Wagner. "It showed us we could accurately take fingerprints from a mobile device and gave our officers the capability to do law enforcement and biometric queries on a smart phone if they saw that an individual requires further investigation."

## Biometric success story

As a law enforcement tool, the Biometric Exit Mobile has produced stunning results. Case in point is an incident that occurred in May at Chicago O'Hare International Airport involving a Polish national couple who were boarding a flight to Berlin, Germany. When the couple presented their passports at the departure gate, the CBP officers didn't find any U.S. visas or country entry stamps, so they decided to run a check and swiped the couple's passports. The biographical information didn't reveal anything derogatory, but as a precautionary check, the officers used the Biometric Exit Mobile device to take the couple's fingerprints. The officers took the index prints of the woman first and within seconds, she came back as a watchlist hit. The same occurred with the man. Both had been ordered deported by an immigration judge, but they didn't leave the country.

The officers wanted to clarify what they discovered, so they reached out to a colleague. "I pulled up the woman's name and nothing came up. There was no record on her whatsoever," said Jonathan Cichy, a CBP enforcement officer who works outbound operations at O'Hare Airport. "However, when I checked her fingerprints, there was a hit, but for a woman with a different date of birth and a different identity, which she had been arrested and deported under."

Then Cichy looked at the manifest for the flight. "I saw they weren't on it. There was no record of the identities they were using to get on the plane," he said. After checking further, Cichy found that both of the Polish nationals had criminal histories with multiple identities. "But none that came up in our systems because they weren't leaving under any of those identities. Biographics alone did not tell us the full story," said Cichy, who quickly rushed to meet the flight that was leaving in 20 minutes.

The couple was allowed to board the flight, but not until Cichy had served them with legal papers to verify their departure and close out the deportation case. "If either one of them is found attempting to return to the U.S. without permission, they could be prosecuted for reentry after deportation, a felony that carries a sentence of two to 20 years," said Cichy.

## Decisive moment

CBP's biometric exit tests culminated in June 2016 with a pilot program at the Atlanta airport. Wagner and his team had a breakthrough. All the work they had done for the past several years was finally coming to fruition. "We came up with a way of taking the information we receive about passengers from the airlines and matching it against information we already have in our government databases," said Wagner.

Based on their research, Wagner and his team decided to use facial recognition technology. "We found that facial recognition was intuitive for people. Everybody knows how to stand in front of a camera and have his or her picture taken. Not so with iris scans and fingerprints. Every time a traveler does the process wrong, someone has to instruct him or her the right way to do it," said Wagner. Aside from being quicker than other biometric methods, facial recognition had additional pluses. The physical design of the camera didn't take up much space, and the equipment wasn't costly. Furthermore, CBP already had a collection of photos for biometric comparison. "People have already provided their photographs to the government for travel purposes," said Wagner.

CBP started testing biometric facial recognition technology on departing overseas flights with Delta Air Lines in June 2016 at Hartsfield-Jackson Atlanta International Airport. Above, CBP Officer Ernesto Julien, right, assists passengers as they scan their boarding passes and have their photos taken before boarding a flight to Mexico City. Delta Air Lines Senior Agents Maribel Marcano, center, and Garrick Ealey, far right, welcome passengers aboard the flight. Photo by Rob Brisley

But the real feat was when CBP found a way to speed up the photo matching process. "As soon as a passenger checks in with the airline, the airline tells us who is getting on the plane. At that point, we find all the photographs we have of the people on the flight and we pool them, and then segment them into individual photo galleries for each passenger," said Wagner. "If there are 300 people on the flight, we find every photograph we have of those 300 people. Generally, that means we will have about 1,500 pictures because we have multiple photos of each passenger."

Then, as the passenger boards the flight, he or she has his picture taken. That photo is compared to his or her individual gallery of photos rather than comparing it to a billion photos that are in DHS's biometric database. "The matching is done in real-time because it's a small file and it's accurate," said Wagner.

The Atlanta pilot also was designed with certain parameters. "We did not want to add another layer onto the travel process," said Wagner. "We told our stakeholders, 'We want to design something that fits within your existing operations and infrastructure. We're trying to make things easier for travelers. We don't want to add additional steps or processes.'"

## Strong partnership

Wagner reached out to Delta Air Lines to see if they would work on the pilot and the airline agreed. "We have a very strong, long-standing, collaborative relationship with CBP," said Jason Hausner, Delta Air Lines' director of passenger facilitation. "Normally, when they approach us to do something, we're in. We like to be in on the front end to provide our expertise and help shape things."

Delta also had a long-range vision of using biometrics for its own operational purposes. "When we heard the proposal from CBP to test biometric exit technology, it resonated with us because one of the elements we were looking at is biometric boarding," said Hausner.

In February 2016, Delta met with CBP to develop a project plan and decided to test a flight from Atlanta to Tokyo, Japan. The pilot, which began in June, was successful, so by September, CBP decided to test another flight with a different demographic. This time the flight was to Mexico City. "We didn't expect a lot of enforcement activity on the Tokyo flight. Years of clearing that flight inbound have shown a very low rate of enforcement violations," said Kevin Pfeifer, CBP's assistant port director of tactical operations at the port of Atlanta. "With Mexico City, we have a history of encountering enforcement violations on inbound flights, so we really expected to see the same percentage outbound and that's exactly what we've seen."

After more than a year of testing, the facial recognition technology has consistently shown a high rate of accuracy. "Our percent of successful matches is in the high 90s. It's even moved up a notch in terms of quality and accuracy," said Nael Samha, CBP's director of passenger systems who built the architecture for the pilot's operating system.

Operationally, the pilot has performed well too. "One of the things we wanted to evaluate was the impact on our operations. Would it delay boarding? Would it impact our on-time performance? We're very metrics oriented," said Hausner. "So far, this test has not impacted us in any manner, and part of it is because of the approach that CBP has taken. They know that in order for their program to be successful, they need to partner with us."

## Industry innovations

During the summer of 2017, CBP conducted technical demonstrations of the biometric exit facial recognition technology with various airlines and airports throughout the country. "We wanted to show stakeholders and the public what this technology is, how it works, and explore how biometric exit technology can fit into airline and airport business models and modernization plans," said Wagner.

Some airlines are already making headway. At JFK and in Atlanta, Delta is testing ways to combine the facial recognition technology with its boarding pass procedures. "The CBP pilot is a two-step process by design, but it seemed to us that when this is implemented across the country, it should be a one-step process," said Hausner.

In June, JetBlue Airways transformed this goal into a reality and was the first airline to board passengers using biometric facial recognition instead of boarding passes. Unlike the technical demonstrations that CBP was conducting with other carriers, JetBlue proposed the pilot. The airline wanted to design its own technology and incorporate it with CBP's facial recognition matching system. "CBP was very open-minded with what we wanted to accomplish," said Liliana Petrova, JetBlue Airways' director of customer experience. "They flew out to Boston and spent several hours with us and took the time to listen. We wanted them to know exactly how we wanted to integrate the biometric technology with the experience at our gate."

The pilot, which was tested at Logan International Airport in Boston, was assembled very quickly. "CBP gave it priority and helped us do a very fast buildout," said Petrova. "Not many partnerships, even private partnerships, function as smoothly."

According to Petrova, the biometric system is part of JetBlue's strategy to remove the hassle from the traveling experience. "Passengers don't have to stop, look for their boarding passes or their IDs. The line moves faster and they don't have to wait as long," she said. "We're trying to take the anxiety out of flying and allow our crew members to interact more with customers."

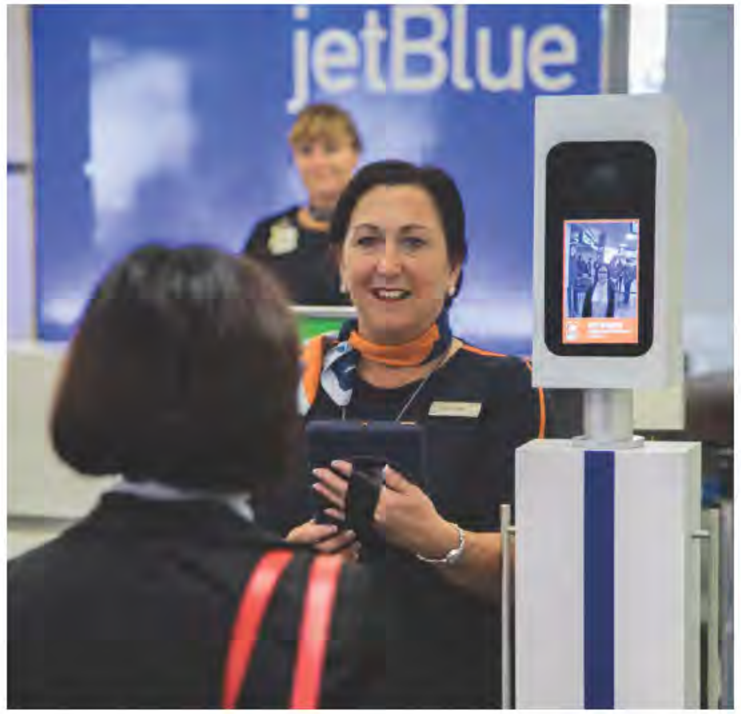
JetBlue's customer feedback was positive. "The customers are really delighted by it. They think it's cool and they're having fun," said Petrova. As a result, JetBlue has decided to expand the pilot in late 2017 with additional flights departing from Boston and JFK.

CBP's future vision for biometric exit is to build the technology nationwide using cloud computing. "There are hundreds of airports throughout the U.S. where we provide services for international travelers and we still need to work through the deployment schedule and timeline," said Wagner. "We also need to determine the technology we'll use. We've been working with airports and airlines to arrive at some of those answers. We want them to tell us what the equipment should look like, so that it fits in with their operational needs."

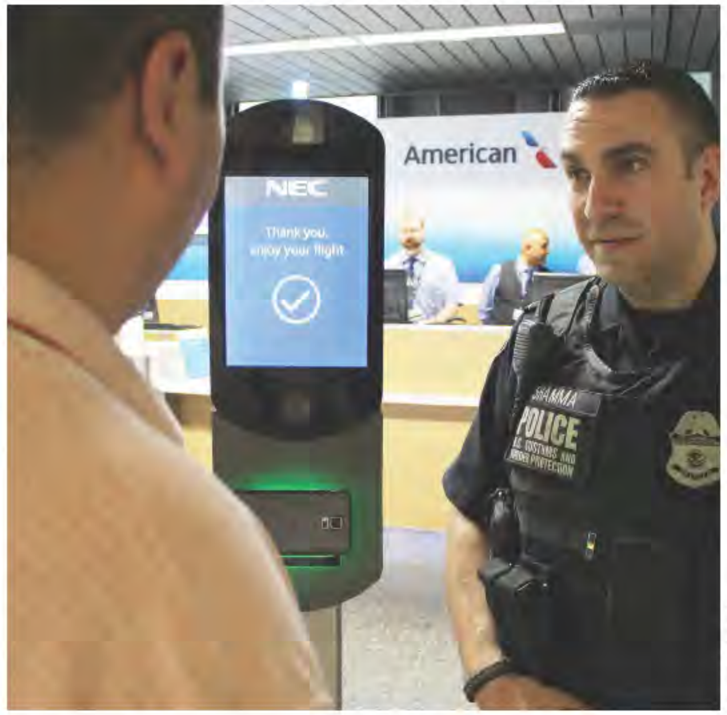
Plans are also underway to update CBP's biometric inbound technology. "We'll be using the same system for our arrivals processing as we do for biometric exit," Wagner explained.

But that's not all that CBP has in store. "We're also looking at communicating with people on their mobile devices as they deplane," said Wagner. "If we can give travelers better guidance on how to navigate customs and the maze at the airport, we can increase efficiency and give them peace of mind."

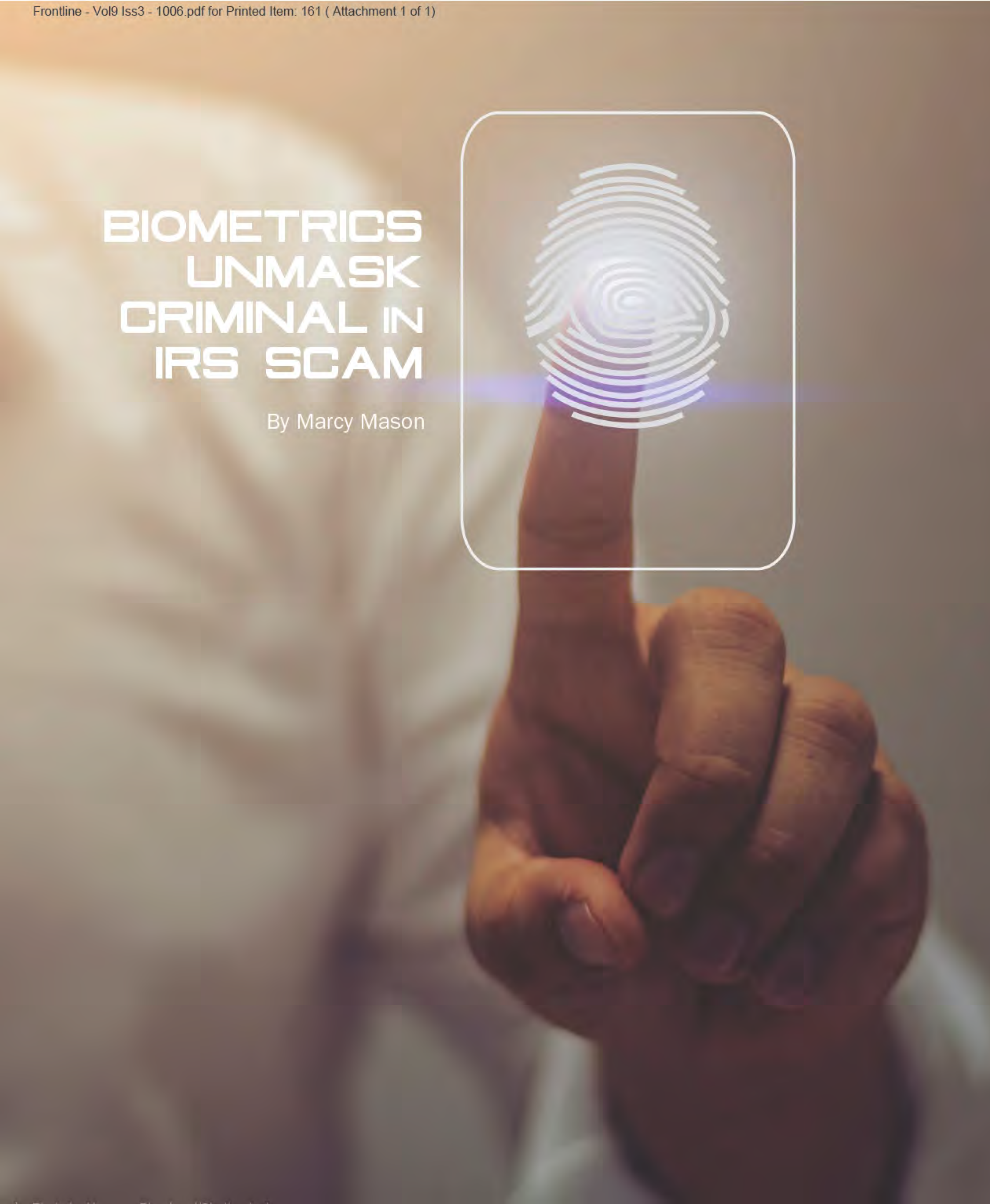
Atlanta Assistant Port Director Kevin Pfeifer, left; Walter Jung, Delta passenger service associate, center; and CBP Watch Commander Marvin Chargualaf discuss biometric testing on international flights at Hartsfield-Jackson Atlanta International Airport. Photo by Ozzy Trevino



JetBlue was the first airline to incorporate its own biometric technology with CBP's facial recognition matching system to verify passengers exiting the U.S. A pilot program using the technology was launched in May 2017 at Logan International Airport in Boston. Photo by Zack Caplan



During the summer of 2017, CBP conducted biometric exit facial recognition technical demonstrations with various airlines and airports throughout the country. Here, CBP Officer Michael Shamma answers a London-bound American Airlines passenger's questions at Chicago O'Hare International Airport. Photo by Brian Bell



# BIOMETRICS UNMASK CRIMINAL IN IRS SCAM

By Marcy Mason

An extraordinary example of how biometric exit technology is enhancing CBP's enforcement capabilities happened in April at Chicago O'Hare International Airport. A 38-year-old, Indian national, Dipakkumar Patel, presented an emergency Indian passport to board a flight to Abu Dhabi, United Arab Emirates, where he was making a connection to India.

While inspecting the passport, the CBP officer at the departure gate didn't find a U.S. visa and the pages of the passport were blank. There wasn't a U.S. entry stamp. When questioned, Patel told the officer that he had entered the country illegally through Mexico six years earlier. The officer decided to call CBP's Passenger Analysis Unit and asked them to run the man's name through the law enforcement databases to check if he was on a watch list.

A name came back with 22 aliases, and Patel's name was one of them. But it was a common Indian name and the match wasn't conclusive. So the officer decided to do a biometric check and called his colleague to come to the jet bridge to take Patel's fingerprints. Using CBP's Biometric Exit Mobile device, a handheld, biometric tool, the officer swiped Patel's passport and took prints of his two index fingers. "All of our systems were queried and within seconds it came back that he was a biometric match," said Jonathan Cichy, a CBP enforcement officer who works outbound operations at O'Hare Airport.

"He came into the country as a Portuguese national using one identity and was leaving the U.S. as an Indian national using another," said Cichy. "The Portuguese passport was legally issued to him, but he had obtained it fraudulently."

And there was more. When Patel's name was matched to one of the aliases, an alert was sent to CBP's National Targeting Center, the Department of Homeland Security's Office of Inspector General, and Homeland Security Investigations. "Patel was linked to a call center scheme where U.S. citizens had been defrauded out of hundreds of millions of dollars in unpaid taxes," said Cichy. All three authorities requested that CBP detain Patel and stop him from getting on the flight.

Patel was turned over to U.S. Immigration and Customs Enforcement and was placed in a local holding facility. He remained there until investigators from the DHS Office of Inspector General and HSI arrived to interview him. Patel was arrested on charges of passport fraud and, in May, was indicted by a grand jury in Atlanta, where he was taken to await his trial. In 2012, Patel had entered the U.S. through Atlanta, using the fraudulently obtained Portuguese passport.

In August, Patel pleaded guilty to a slew of crimes. In addition to false use of a passport, he plead guilty to a conspiracy charge for his role in a multimillion-dollar India-based call center scam that targeted U.S. victims. According to his plea, Patel and his co-conspirators perpetrated a complex scheme in which individuals from call centers located in Ahmedabad, India, impersonated officials from the IRS and U.S. Citizenship and Immigration Services to defraud victims throughout the U.S. The victims were threatened with arrest, imprisonment, fines or deportation if they did not pay the money they allegedly owed the government. Victims who agreed to pay the scammers were instructed to provide payment using prepaid credit cards or wiring money. Upon payment, the call centers would immediately turn to a network of "runners" based in the U.S. to liquidate and launder the fraudulently-obtained funds. Patel served as a runner.

"Without the use of biometrics, Patel would have been allowed to depart the U.S. and return to his home country. He would not have been linked to any of the fraud that he committed against the U.S. and our citizens," said Cichy. "Biometrics are a critical tool in law enforcement. They reveal a person's true identity and help us protect America." F

Photo by Urupong Phunkoed/Shutterstock.com

# A HISTORY OF INNOVATIVE TECHNOLOGY

By Marcy Mason

At the same time that CBP was focusing on biometrics, the agency was developing technology that would expedite the processing of travelers and reduce wait times in airports. Air travel was growing, and by all indications, that trend would continue. According to the International Air Transport Association's latest projections, air travelers will double over the next 20 years.

In 2007, when CBP introduced Global Entry, it was an innovative concept because it was directed at low-risk travelers. "Global Entry was designed to give low-risk, frequent travelers the ability to use technology to expedite their arrival process," said Dan Tanciar, CBP's deputy executive director of planning, program analysis, and evaluation for entry/exit transformation. "The program allowed us to identify low-risk travelers, so that we could focus our attention on the travelers we don't know much about."

A few years later, in 2012, CBP launched another innovation—a self-service kiosk that helped speed up the traveler inspection process. The kiosks, known as Automated Passport Control, performed the administrative steps that CBP officers had traditionally handled, so that officers could focus more on inspections. The kiosks also enabled CBP to do away with paper forms, allowing travelers to submit their declaration and biographic information electronically. "Within two years, we were able to deploy about 1,500 kiosks at all of the top airports throughout the U.S. and we reduced wait times by about 30 to 35 percent," said Tanciar. "The Automated Passport Control kiosks shortened the amount of time travelers spent with CBP officers from 3 minutes to 30 to 60 seconds."

Automated Passport Control kiosks, another CBP innovation, speed up the traveler inspection process by performing administrative steps CBP officers previously handled. At the Miami International Airport, shown above, the self-service kiosks were initially installed as a way to process travelers faster during the 2014 FIFA World Cup. The technology shortens the time inbound travelers spend with CBP officers from 3 minutes to 30 to 60 seconds. Photo by Manuel Garcia

## Economic impact

With CBP's staffing limitations, the success of the technology was paramount. Not just for CBP, but for its air industry partners too. "Airports are economic generators for their communities, so if you reduce the capacity of the airport, in effect, you're reducing the economic capabilities of the airport for its community," said Matthew Cornelius, vice president of air policy for Airports Council International-North America, a trade organization that represents airports in North America.

In 2013, when the Automated Passport Control kiosks were starting to appear at U.S. airports, Airports Council International saw the value of the technology and wanted to expand it. "We were approached by one of our associate member companies, Airside Mobile, a tech firm, that had a concept to create the same functionality of the kiosks, but to do it on a smartphone," said Cornelius. In other words, international travelers could fill out the required customs information on their smartphones before they ever got off the plane. "We saw it as an opportunity to alleviate some of the problems our members were having at their international arrival facilities. We knew that mobile applications and mobile technology are really the wave of the future."

Cornelius took the concept to CBP. "We told CBP, 'We have this idea. We think it's going to be helpful. Will you work with us on it?' To CBP's credit, they saw it made sense, that it was going to help us do our jobs better and alleviate the problem of processing travelers into the U.S," said Cornelius.

CBP and Airports Council International began piloting the Mobile Passport Control app in August 2014. A year later, the pilot expanded to five airports. Today, 24 airports and one cruise port use the app and it has been downloaded more than 2.4 million times.

"It's a great example of partnership. We worked very closely with CBP," said Cornelius. "Everybody was on board, understood what needed to be done, and it all came together perfectly."

## Faster processing

The technology was also critical for the airlines. "In early 2014, we knew the World Cup was being played in Brazil that year, so that meant there would be a lot of travel through Miami," said Howard Kass, American Airlines' vice president of regulatory affairs. "We knew that the processing times and the facilitation in Miami weren't what we wanted them to be. It wasn't a good customer experience," he said.

"The lines were long. There were multi-hour waits, and we felt the brunt of it because when travelers landed, they couldn't move through customs, so they misconnected on their flights," said Kass. "We then had to figure out how to get them to their destinations or put them up in a hotel. We spent lots of money to ameliorate the misconnections. Miami was getting a bad reputation among travelers, which is something we don't want to see at any of our hubs."

The airline thought CBP's technology might be the answer. "We knew from what we'd seen in other airports that the machines would be a tremendous benefit in Miami to help expedite people through the process," said Kass. So American Airlines worked with CBP and the Miami International Airport to get more Global Entry and Automated Passport Control machines in place. "We more than doubled the number of machines and we did a lot of marketing, advertising, and inflight announcements to encourage passengers to use the technology, so they could be processed quickly through the CBP facility," said Kass.

And it worked. "We got to a point where every U.S. citizen was using some kind of automation," he said. "CBP pledged a lot of resources to make sure that flights were processed smoothly during the World Cup. It was important to the United States that there wasn't a rough spot in Miami with all the traffic moving through." Moreover, said Kass, "There weren't any meltdowns or passengers stranded for hours and hours in the terminal and we made some improvements that really helped travelers move through the process more quickly."

CBP officers and representatives from many law enforcement agencies at the National Targeting Center work together to counter terrorism and criminal activities.

# WORKING TOGETHER

## CATCHING SMUGGLERS, TERRORISTS AND LAWBREAKERS WORKS BETTER THROUGH PARTNERSHIP

By Paul Koscak, photos by Glenn Fawcett

Since 2001, CBP's National Targeting Center in Sterling, Virginia, has worked nonstop to catch travelers and detect cargo that threaten our country's security. At the same time, the center is working just as hard to build a network of partner nations committed to fighting global threats. Increased targeting by all partners increases security for all is the concept.

That principle also supports the United Nations Security Council's Resolution 2178 requiring member nations to fight international terrorists and criminals by strengthening laws to prosecute them and requiring airlines to provide passenger lists. The resolution also calls for member nations to share information that can alert any partner nation, including the U.S., to an identified threat.

But effective passenger vetting hinges on the quality of a nation's risk assessment system. Some nations don't even have automated systems and manually comb through the data. At times, the enormous flow of cargo and passengers can overwhelm available resources.

To overcome these limitations, CBP offers its automated targeting system-global or ATS-G software along with technical assistance, to potential partners. ATS-G is similar to the software used at the Office of Field Operations's (OFO) National Targeting Center and evolved from decades of experience designing and operating passenger and cargo targeting systems. The software can vastly improve how travelers flying in and out of a country are vetted.

ATS-G rapidly compares passenger and cargo manifests against data bases and other records for clues that could reveal a high-risk traveler, such as a foreign terrorist.

The package includes a free software license, free installation tailored to a partner's needs as well as technical support and training. "We follow up two or three times per year to ensure the system is running and provide training on how to target," said Jerry Kaplan, ATS-G assistant director.

Use of ATS-G by foreign partners also supports the tenets of resolution 2178. ATS-G is part of a larger program of technology assistance, law enforcement and border security relationships.

New Zealand is one partner using ATS-G. Tony Davis, manager of New Zealand's Integrated Targeting and Operations Centre, said the software is user friendly, allowing the center to switch from screening flights—one at a time—to vetting passengers hundreds at a time. "ATS-G is fantastic and it's our primary targeting tool," he said. "CBP support has been excellent."

Sharing information with the U.S. and other countries, creates a bond that builds relationships, added Craig Chitty, manager of operations at the center. "It's very advantageous because it builds trust," he said.

Other nations have noticed and frequently contact the center to learn more about the software. "I'm a salesman for ATS-G," Chitty remarked. "We get approached by international organizations on the phone or by visits."

## Another option

Gaining partners can be challenging. Political or legal roadblocks regarding sovereignty prevent some nations from freely collaborating with the U.S or other nations, explained NTC Director Troy Miller. For those countries, CBP created the global travel assessment system or GTAS. GTAS permits foreign countries to independently perform vetting activities without the collaboration involved with ATS-G.

Launched in 2016, GTAS is free and designed for rapid use. The software is easily downloaded from

CBP Officer Zule Baker reviewing passenger manifest data at the National Targeting Center.

a special CBP website and ready to use. It can also improve an existing vetting system because the coding allows nations to customize the software or just download the portions that meet their needs.

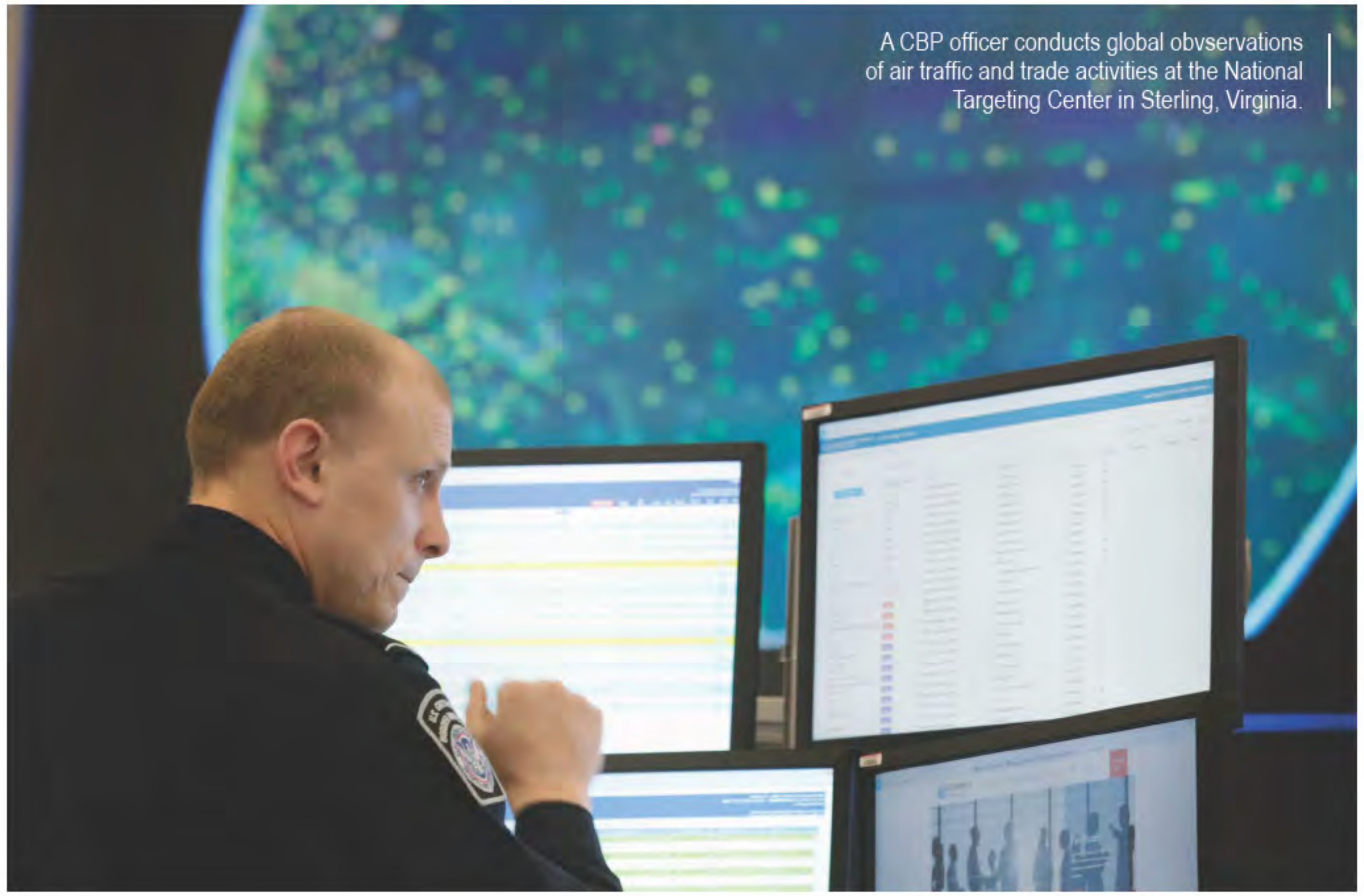
GTAS is comparable to ATS-G because GTAS also automatically evaluates passenger manifests in real time to identify suspicious travelers or crewmembers who may pose a national security risk, justifying a closer assessment. Using GTAS, governments can screen suspects before they enter or leave that nation.

"GTAS also gives them [nations] the ability to comply with the U.N. resolution," NTC Executive Director Troy Miller said.

Since the software is new, CBP is working through the World Customs Organization in Brussels, a group that promotes trade and supply chain security, to spread the word. With 182 members—mostly developing nations with limited resources—GTAS can be an ideal product.

In July, Acting Commissioner Kevin McAleenan sent a letter to the organization outlining the details and benefits of the software. As an added advantage, he said "CBP is willing to provide installation instructions, administration guides and user manuals, as well as technical and subject matter expertise on an ongoing basis…" One nation has already signed up for GTAS, so the outreach is beginning to pay off.

CBP pursues partnerships and promotes ATS- G and GTAS through international forums and events, many of which the U.N and the European Union take part. When international partners are better able to identify possible high risk travelers, they close gaps in terrorist and criminal activities so governments can work together to detect, deter and defeat these threats. In an interconnected world, it is more important than ever that countries conduct these risk assessments, and CBP is helping advance global security through ATS-G, GTAS, and the expertise of the NTC.



A CBP officer conducts global obvservations of air traffic and trade activities at the National Targeting Center in Sterling, Virginia.

# MOVING TARGETS:

## CBP'S AGRICULTURE SPECIALISTS' LATEST SECRET WEAPON

By Kathleen Franklin

An agriculture inspection specialist with CBP Office of Field Operations, National Agriculture Cargo Targeting Unit, inspects containers of imported goods for invasive insect and plant species at the Port of Baltimore. Photo by Glenn Fawcett

Alix Garnier crawls out from under a steel shipping container of aluminum coils at the Baltimore seaport, gingerly holding a glass vial between his thumb and forefinger. The agriculture specialist for U.S. Customs and Border Protection squints at the tiny object inside.

Nearby, Garnier's colleague, CBP Agriculture Specialist (CBPAS) Timothy Morris, has found mollusks on the exterior of the same cargo container. One of the snails was identified as an Amber Snail (Succineidae, sp.)—and that's enough to warrant sending the container back to South Africa.

A few miles inland, at the CBP Centralized Examination Station, CBPAS John Taylor is lying on the ground with a flashlight, peering underneath and through the slats of rough wooden pallets that hold stacks of terra cotta flower pots. At this moment, he's more worried about seeds than splinters.

One of CBP's many important responsibilities is to prevent potentially harmful or dangerous plant and animal material from entering the U.S. This includes insect pests, invasive plants, plant pathogens, and prohibited animal products that could be carrying diseases that could hurt U.S. livestock or humans.

In fiscal year 2016, CBP agriculture specialists conducted more than 9,800 cargo inspections at the Baltimore seaport.

The primary commodities that come through the port are salt, automobiles, sugar, gypsum, plywood, paper, iron ore, oil, and aluminum. Most of these commodities seem like they would be fairly low-risk for agriculture violations—compared to the tons of cut flowers that arrive in Miami, for example.

But Garnier and Taylor know all too well that some dangers are lurking in—and on—the containers themselves, or in the ubiquitous wooden shipping pallets. In fact, of CBP's 328 international ports of entry, the Port of Baltimore ranks number one in general cargo "reportable" pests – those that are reported to the U.S. Department of Agriculture.

An intercepted seed of a tridax daisy, or coatbutton (*Tridax procumbens*), found on a maritime shipment of metal products at the Port of Baltimore.

The plant is a Federal Noxious Weed and has pest status in nine states. Photo by Glenn Fawcett

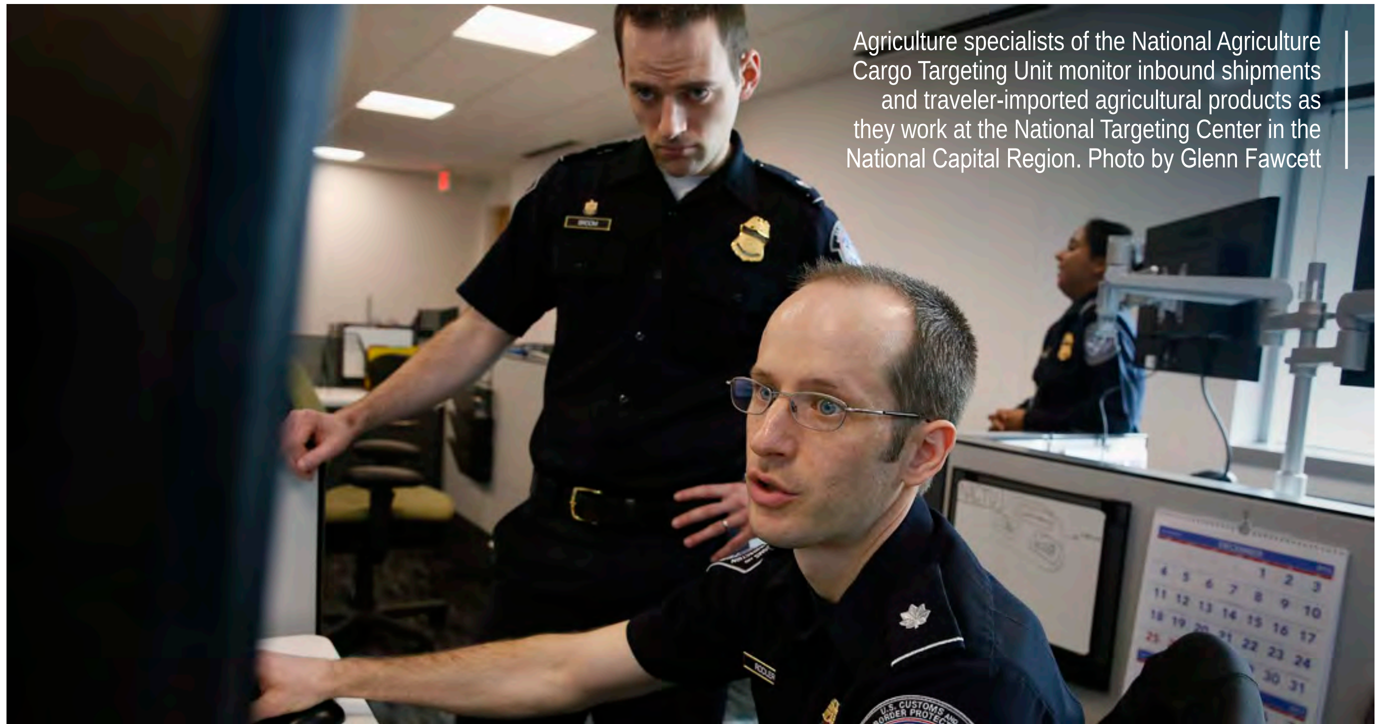
Meanwhile, 55 miles southwest of where Garnier, Morris, and Taylor are working, in a highly secure state-of-the-art office building in Northern Virginia, five specially trained agriculture specialists are scanning screens to see what sorts of agriculture cargo are on its way to our nation's 328 land, air, and sea ports of entry. They occupy just a tiny corner of a vast open sea of hundreds of desks staffed by experts on counterterrorism, immigration admissibility, and other specialized disciplines aimed at securing the U.S. border.

Welcome to the National Agriculture Cargo Targeting Unit, or NACTU. These analysts provide key intelligence to frontline agriculture specialists like Garnier and Taylor, letting them know if a shipment warrants further scrutiny.

The NACTU researches cargo shipments being imported to the U.S. and analyzes national agriculture quarantine activity to identify shipments that pose a significant risk to U.S. agriculture and natural resources. These potential threats include animal pathogens that could harm livestock and people; invasive plants that could damage our ecosystems; and insect pests and plant diseases that could hurt crops and forests.

## Identifying the need

The idea for creating a targeting unit specifically on agriculture cargo originated nearly a decade ago, but efforts got under way in earnest in 2014 when the CBP Office of Field Operations' Agriculture Programs and Trade Liaison office contacted CBP's National Targeting Center, or NTC, to explore options for piloting the unit and collocating it at the cargo portion of the NTC's facility outside Washington, D.C.



Agriculture specialists of the National Agriculture Cargo Targeting Unit monitor inbound shipments and traveler-imported agricultural products as they work at the National Targeting Center in the National Capital Region. Photo by Glenn Fawcett

"We assembled a working group of subject matter experts from various field offices and worked closely with NTC advisers to develop plans to pilot a unit," recalled Supervisory CBP Agriculture Specialist Nikki Thomas, one of the founders of the NACTU. CBP conducted six pilot cycles before establishing the NACTU as a permanent, full-time unit in September 2015 as part of the Agriculture Safeguarding Unit.

The five permanent NACTU targeters are led by Branch Chief Nidhi Singla, and they receive assistance from interns who rotate in from the field, bringing valuable knowledge and expertise with them about trends they see developing at the ports of entry.

"The goal is to cross-pollinate knowledge we have residing in the field with that of our permanent targeters here in NACTU, and then to send them back to the ports with the knowledge they receive here," says Singla.

The targeters have varied backgrounds and experience. For example, after earning a bachelor's degree in biology, Agriculture Operations Manager Samuel Broom interned with U.S. Fish and Wildlife Service in New Hampshire, researching the spawning habits of Atlantic salmon, and then tracking desert tortoises in the Mojave Desert for the U.S. Geological Survey.

"We focus not just on agriculture materials themselves—fruits and vegetables and animal products that could harbor pests and diseases—we also look at the miscellaneous commodities that are also capable of harboring pests and pathogens, such as wood packaging materials like pallets, as well as tiles and even steel," says Singla.

Shipments are sent from the Baltimore seaport to the examination station if CBP believes they merit further inspection. At the station warehouse, agriculture specialists are inspecting a shipment of nails from China—packed on wooden pallets. The reason for the referral: targeters had information indicating the shipment may be contaminated with a weed seed of Imperata cylindrica, or cogongrass, which is classified as a federal noxious weed, or FNW.

Many types of weed seeds—like those of cogongrass—have feather-like protuberances that serve as "wings" when the wind blows, carrying them to other areas—often sticking to the rough wood of shipping pallets. The production of seeds is seasonal, so certain times of year are worse than others in terms of interceptions, depending on the country of origin.

## Finding the target

The targeters who work for the NACTU need the tenacity of private investigators and the patience of stakeout cops. They must be detail oriented and willing to trace the path of a shipment—not just the physical trajectory of the actual cargo, but the paper trail itself.

For example, a shipment from a certain country might list a major city as the cargo's origin because that is the manufacturer's headquarters location. But the materials may have actually been grown, processed, or packed in a remote part of the country where noxious weeds such as wild sugarcane (Saccharum spontaneum) grows. Wild sugarcane is an important habitat for certain animal species, and it is often harvested to thatch roofs.

But here in the U.S., wild sugarcane can quickly colonize disturbed soil to take over fields and pastures, choking out native grasses and crops. In fact, wild sugarcane is on the FNW list, along with cogongrass and more well-known nuisances like mile-a-minute vine (Mikania micrantha Kunth) and kudzu (Puerara montana). Deliberate importation of it is prohibited without a permit from the USDA's Animal and Plant Health Inspection Service.

The NACTU targeters know this. So based on the trends they see—and patterns of deception—they